VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

MODERNÍ CLOUDOVÁ ŘEŠENÍ V PODNIKU
MODERN CLOUD SOLUTIONS IN THE ENTERPRISE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Lenka Fialová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Jiří Kříž, Ph.D.**
SUPERVISOR

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/16
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Lenka Fialová

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách, ve znění pozdějších předpisů, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských, magisterských a doktorských studijních programů zadává diplomovou práci s názvem:

Moderní cloudová řešení v podniku

v anglickém jazyce:

Modern Cloud Solutions in the Enterprise

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

DANIEL, Joshua, Fadi EL - MOUSSA, Gery DUCATEL, Pramod PAWAR, Ali SAJJAD, Robert ROWLINGSON a Theo DIMITRAKOS. Integrating Security Services in Cloud Service Stores. Springer International Publishing, 2015.
MARSTON, Sean, Zhi LI, Subhajyoti BANDYOPADHYAY, Juheng ZHANG a Anand GHALSASI. Cloud computing — The business perspective. Decision Support Systems, 2011. ISSN 0167-9236.
SAVILL, John. Mastering Microsoft Azure Infrastructure Services. Somerset: Wiley, 2015. ISBN 9781119003274.
SODOMKA, Petr. Informační systémy v podnikové praxi. 1.vyd. Brno: Computer Press, 2006. ISBN 80-251-1200-4.
VELTE, Anthony T., Toby J. VELTE a Robert C. ELSENPETER. Cloud computing: praktický průvodce. 1.vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3333-0.
WHEELER, Aaron a Michael WINBURN. Cloud Storage Security: A Practical Guide. Elsevier Science, 2015. ISBN 9780128029305.

Vedoucí diplomové práce: Ing. Jiří Kříž, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/16.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

L.S.

doc. RNDr. Bedřich Půža, CSc.
Ředitel ústavu

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Děkan

V Brně, dne 29. 2. 2016

Abstrakt

Tato diplomová práce se zabývá využitím cloudového řešení v konkrétním podniku. Hlavním cílem práce je výběr systému, který umožní sdílení a synchronizaci dat mezi zaměstnanci a návrh jeho nasazení s ohledem na potřeby analyzované firmy. V rámci práce je také vypracována situační analýza podniku, studie příležitosti a analýza rizik.

Abstract

This diploma thesis deals with the use of the cloud in a particular company. The main objective is to select a system that enables sharing and synchronizing data between employees and to prepare a proposal to deploy the system with regard to specific needs of the analyzed company. As part of the work is also the situation analysis, opportunity study and risk analysis.

Klíčová slova

Cloudový systém, Cloud Computing, ownCloud, analýza rizik, cloudové úložiště, sdílení dat v podniku

Keywords

Cloud system, Cloud Computing, ownCloud, risk analysis, enterprise data sharing

Citace

FIALOVÁ, L. *Moderní cloudová řešení v podniku.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 75 s. Vedoucí diplomové práce Ing. Jiří Kříž, Ph.D.

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracovala sama pod vedením Ing. Jiřího Kříže, Ph.D.

. . . . . .

Lenka Fialová

26. května 2016

Poděkování

Chtěla bych poděkovat Ing. Jiřímu Křížovi, Ph.D. MBA za odborné vedení této práce. Děkuji také rodině a partnerovi za podporu během studia.

Obsah

1 Úvod

Tato práce se zabývá problematikou cloudových řešení. Cílem práce je výběr a návrh cloudového systému pro konkrétní podnik. Nový informační systém má usnadnit zaměstnancům vzájemnou komunikaci, vyřešit synchronizaci, ukládání dat a umožnit práci na sdílených dokumentech. Speciální důraz je kladen na zvýšení zabezpečení firemních dat, tedy aby se podniková data nacházela přímo na serveru, který má firma k dispozici.

V kapitole 2 jsou představeny všechny dílčí cíle této práce, dále je popsán postup zpracování a metody, které byly použity. Kapitola 3 je věnována teoretickým východiskům. Kromě vysvětlení základních pojmů z oblasti cloudu, je zde krátký náhled do historie Cloud Computingu, jsou popsány výhody, nevýhody i rizika používání cloudu. Navazuje na ni kapitola 4, kde je představen podnik, který má zájem o využití cloudu pro zefektivnění práce svých zaměstnanců. V této kapitole je rovněž vypracována studie příležitosti, která je podkladem, zda doporučit nasazení nového systému ve firmě. Na závěr kapitoly jsou definovány požadavky podniku na informační systém. Následující kapitola 5 se zabývá samotným návrhem řešení. V úvodu kapitoly jsou porovnána vhodná řešení a je vybrána technologie výsledného systému. Poté následuje podrobnější popis zvoleného řešení, je uveden postup instalace a konfigurace systému dle potřeb podniku. V závěru kapitoly je zpracována riziková analýza, která vyhodnocuje hrozby související s novým systémem a zahrnuje návrh opatření snižující úroveň stanovených rizik. Závěrečná kapitola 6 shrnuje výsledky této práce.

2 Cíle, postup zpracování a metody

Obsahem následující podkapitoly 2.1 je stanovení cílů této práce. V další podkapitole 2.2 je popsán postup vypracování včetně krátkého popisu metod, kterých bylo využito.

2.1 Cíle

Hlavním cílem této práce je vypracování postupu nasazení systému ve firmě, která projevila zájem o cloudové řešení pro sdílení a synchronizaci dat mezi svými zaměstnanci. Dalším cílem je zaanalyzovat rizika hrozící při nasazení cloudu v podniku a navrhnout pro ně patřičná opatření.

Sekundárním cílem je vysvětlit základní pojmy související s problematikou cloudu, dále rozhodnout, zda je nasazení cloudu pro firmu přínosné a vybrat z dostupných technologií nejvhodnější řešení.

2.2 Postup zpracování a metody

Úvodním úkolem při postupu zpracování této práce je nastudování a zpracování teoretických poznatků z oblasti cloudu.

Dalším krokem je zpracování studie příležitosti, z které bude možné určit, zda je změna informačního systému v současnosti pro podnik vhodná. Za tímto účelem je zpracována situační analýza podniku zahrnující analýzu obecného okolí metodou SLEPT, analýzu oborového okolí Porterovou metodou a analýzu interního prostřední metodou 7S. Výsledky zmíněných analýz jsou podkladem pro shrnující analýzu SWOT.

Po zhodnocení vhodnosti projektu jsou uvedeny požadavky, které management podniku klade na nový systém. Na jejich základě je zvoleno několik dostupných alternativ řešení. Navrhované technologie budou vzájemně porovnány a zvolí se nejvhodnější varianta. Dále budou podrobněji rozebrány možnosti vybraného systému s ohledem na firemní strukturu a procesy. Následně je zpracován podrobný návod pro instalaci a konfiguraci zvoleného systému pro potřeby podniku.

Na závěr budou podle metody RIPRAN analyzovány hrozby a navržena vhodná opatření, která povedou k odstranění nebo snížení rizik. Ke grafickému znázornění efektivity stanovených opatření bude využit pavučinový graf a mapa rizik.

2.2.1 Studie příležitosti

Studie příležitosti (Opportunity Study) bývá zpravidla součástí předprojektové fáze. Cílem studie je zvážit současný i budoucí stav situace podniku a určit do jaké míry je vhodné projekt realizovat [1]. K vyhodnocení situace podniku budou využity metody strategické analýzy - analýza vnějšího okolí, analýza oborového okolí a analýza interních faktorů. Na základě výsledků zmíněného průzkumu bude vyhotovena shrnující analýza SWOT a vyhodnocení o vhodnosti realizace projektu.

SLEPT

Jednou z vhodných technik pro analýzu obecného okolí firmy je analýza SLEPT. Smyslem této metody je identifikovat nejvýznamnější vlivy vnějšího okolí, které mají nějakým způsobem dopad na organizaci [3]. Název je akronym a jednotlivá písmena vyjadřují typy vnějších faktorů. Jde o faktory:

- sociální - průmět sociálních vlivů na organizaci, včetně kulturních vlivů a změn,
- legislativní - průmět vlivů národní a mezinárodní legislativy,
- ekonomické - průmět vlivů místní, národní a mezinárodní ekonomiky,
- politické - průmět existujících a potenciálních politických vlivů,

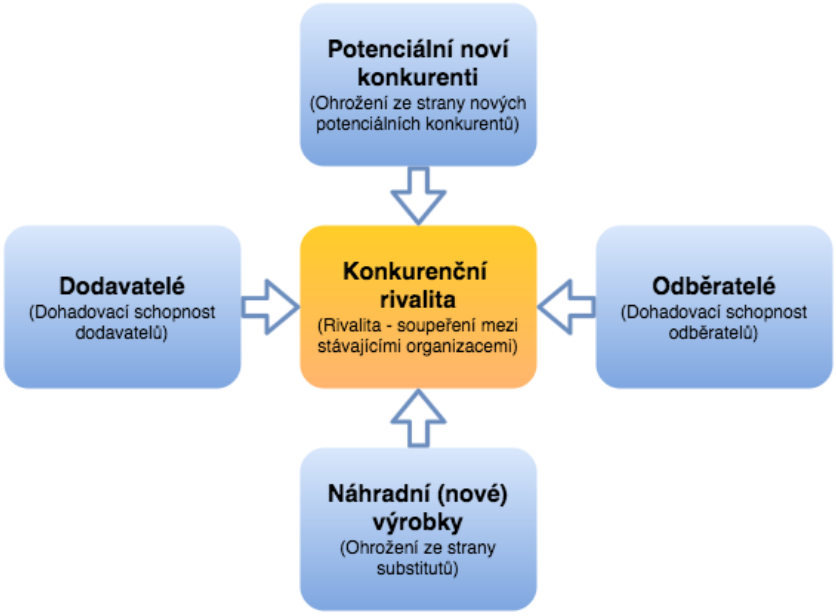
- technologické - průmět vlivů měnících se technologií [2].

Tato metoda existuje ve více variantách, které se mezi sebou liší pořadím faktorů, v literatuře se můžeme tedy setkat také s názvem PESTLE, PEST, STEER, STEP, STEEPLES [3].

Porterova analýza

Porterova analýza je metoda, kterou lze využít pro zmapování situace oborového okolí firmy. Podstatou metody jsou prognózy vývoje konkurence ve zkoumaném odvětví. Model je založen na působení pěti sil, které bezprostředně ovlivňují podnikání na daném trhu. Mezi pět základních sil patří:

- riziko vstupu potencionálních konkurentů,
- rivalita mezi stávajícími konkurenty,
- smluvní síla odběratelů,
- smluvní síla dodavatelů,
- hrozba substitučních produktů [4].



Obrázek 2.1: Působení konkurenčních sil u Porterova modelu [4], vlastní zpracování

Analýza 7S faktorů

Interní faktory firmy lze zjistit metodou „7S faktorů McKinsey“. Jde o analytickou techniku, která se používá pro hodnocení jednotlivých důležitých částí struktury společnosti:

- **strategie** – plánované cíle, které povedou k rozvoji firmy;
- **struktura** – hierarchická struktura společnosti, komunikační kanály mezi odděleními;
- **systémy** – manažerské postupy, informační systémy a technologie;
- **styl** – charakteristický způsob komunikace a jednání mezi zaměstnanci, vystupování společnosti vůči zákazníkům, prostředí společnosti;
- **spolupracovníci** – výběrová řízení, sebevzdělávání zaměstnanců, motivace zaměstnanců;
- **schopnosti** – dovednosti, znalosti, zkušenosti zaměstnanců společnosti a jejich ohodnocení;
- **sdílené hodnoty** – tzv. „nadřazená hodnota“, shrnutí podnikové kultury, vize, poslání, základní hodnoty společnosti [6].

Obrázek 2.2: Propojení faktorů u metody „7S faktorů McKinsey [5], vlastní zpracování“

SWOT

Analýza SWOT se využívá ke komplexnímu vyhodnocení fungování podniku. Díky ní dokážeme nalézt problematické oblasti nebo nové možnosti rozvoje firmy. Termín SWOT je odvozen z počátečních písmen slov:

- Strengths - silné stránky
- Weaknesses - slabé stránky
- Opportunities - příležitosti v okolí firmy
- Threats - hrozby v okolí firmy

Úkolem SWOT analýzy je identifikovat zásadní silné a slabé stránky organizace a klíčové příložitosti a hrozby vnějšího prostředí. Výstupem je matice se čtyřmi kvadranty, do nichž se zmíněné oblasti zájmu zapisují.

Silné stránky (Strengths)	**Slabé stránky** (Weaknesses)
...	...
Příležitosti (Opportunities)	**Hrozby** (Threats)
...	...

Tabulka 2.1: Obecná matice analýzy SWOT, vlastní zpracování

2.2.2 Analýza rizik

Analýza rizik je přirozeně důležitým krokem procesu snižování rizik. Je obvykle chápána jako proces definování hrozeb, pravděpodobností jejich výskytu a závažnosti dopadu [2].

Prvním úkolem v rámci analýzy rizik je jejich identifikace. V této části se snažíme identifikovat nebezpečí, která mohou významně ovlivnit úspěšnost projektu. Dalším úkolem je analyzovat identifikované hrozby a odhadnout pravděpodobnost výskytu určitého nebezpečí a odhadnou výši předpokládaného nepříznivého dopadu na projekt.

Analýza rizik může být:

- **kvantitativní**, pokud hodnota pravděpodobnosti výskytu rizika a hodnota dopadu rizika je vyjádřena číselnou hodnotou;
- **kvalitativní**, pokud ke stanovení pravděpodobnosti a dopadu je užito slovní vyjádření.

Dalším krokem je určení hodnoty rizika, která je vypočítána opět kvantitativně nebo kvalitativně. Cílem je zjistit míru významnosti rizika a určit, která z rizik mají být ošetřena, která mohou být zanedbána, a která nelze akceptovat [1].

Po této fázi přichází na řadu ošetření rizik. Úkolem je zamyslet se, jak reagovat na identifikovaná rizika a navrhnout taková opatření, která by snížila celkovou hodnotu rizik na takovou úroveň, aby byl projekt s vysokou pravděpodobností úspěšně realizovatelný.

RIPRAN

V této práci bude k analýze rizik využito empirické metody RIPRAN (RIsk PRoject ANalysis). Autorem této metody je Branislav Lacko.

Metoda se skládá ze čtyř částí:

1. identifikace nebezpečí projektu;
2. kvantifikace rizik projektu;
3. reakce na rizika projektu;
4. celkové posouzení rizik projektu. [1]

V první části hledáme dvojice hrozba-scénář. Hrozby jsou projevy nebezpečí pro projekt a scénář je děj, který nastane v důsledku výskytu hrozby. Lze využít postup, kdy k hrozbě hledáme možné následky nebo opačný postup, kdy ke scénáři hledáme jeho příčinu.

V další části probíhá kvantifikace rizik. Hodnota rizika se vypočte jako součin pravděpodobnosti scénáře a hodnoty dopadu. U metody RIPRAN lze využít jak verbální, tak číselnou kvantifikaci.

Dalším krokem je stanovení opatření proti zjištěným rizikům.

Podle [1] jsou výsledky rizikové analýzy metodou RIPRAN doporučeny prezentovat v tabulkové nebo textové formě. Pro účely této práce byla vybrána textová forma, u které se doporučuje následující struktura:

Pořadové číslo: **I.**

Hrozba:

Scénář:

Pravděpodobnost:

Dopad:

Hodnota rizika:

Návrh na opatření:

Snížená hodnota rizika:

Závěrečným krokem metody je celkové posouzení rizikovosti projektu a doporučení, zda je vhodné v projektu pokračovat.

3 Teoretická východiska z oblasti Cloud Computingu

Cloud je v posledních letech velice aktuálním trendem v oblasti informačních technologií. Základní ideou cloudu je umožnění vzdáleného poskytnutí služeb prostřednictvím internetu. Přesný výklad pojmu cloudová technologie neboli Cloud Computing nebyl dosud standardizován. V této práci budu čerpat především z definice uznávané většinou odborníků, a to je komplexní definice, kterou nabízí National Institute of Standards and Technology (NIST) ve svém dokumentu „The NIST Definition of Cloud computing“ [7].

V následující podkapitole 3.1 budou popsány cloudové technologie v historickém kontextu. Dále budou v podkapitole 3.2 představeny základní pojmy Cloud Computingu vycházející z definice podle NIST. Naváže samostatná podkapitola 3.3, kde jsou rozebrány výhody a poté nevýhody cloudových řešení.

3.1 Historie

Myšlenku Cloud Computingu poprvé prezentoval v 60. letech minulého století John McCarthy. Sdílení počítačových technologií tenkrát přirovnal ke sdílení elektrické energie. Elektronickou energii využívá mnoho domácností a firem, které mají zakoupeny elektronické spotřebiče. Málokterá domácnost nebo firma si ale kvůli tomu pořizuje vlastní elektrárnu. Mnohem častější je model, kde jednu elektrárnu využívají stovky, tisíce až desetitisíce odběratelů, kteří se k ní připojují vzdáleně – pomocí elektrorozvodné sítě. Tato analogie dokonce postihla i hardwarovou a softwarovou virtualizaci, aniž by v té době existovala. Ve skutečnosti je elektráren v elektrorozvodné síti více než jedna a elektrárny

jsou vzájemně propojeny. V případě výpadku jedné z nich přebírají její zátěž ostatní elektrárny a odběratelé výpadek nepocítí. Ve světě současných počítačů v hlavních metaforických rolích vystupuje datové centrum poskytovatele Cloud Computingu jako elektrárna, internet jako elektrorozvodná síť a počítač jako elektrický spotřebič. V angličtině služby poskytovatelů elektrické energie a jiných veřejných služeb spadají pod souhrnný název utility, proto byla technologie Cloud Computingu v minulosti označována jako Utility Computing [8].

Pojem Cloud Computing poprvé použil až v roce 1997 Ramnatha Chellapa. Pojem „cloud“ neboli oblak je popisné vyjádření, které se používalo ve schématu infrastruktury Utility Computingu. Oblak je historicky využíván ve schématech telekomunikačních sítí, kde koncová zařízení jsou připojená k oblaku vyjadřující internet. Protože Utility Computing s internetem významně operuje, začal se od roku 1997 místo Utility Computing používat název Cloud Computing [8].

Za rozšířením komerčního Cloud Computingu se zasloužily hlavně telekomunikační společnosti, které v 90. letech minulého století začaly poskytovat virtuální privátní sítě (VPN). VPN jim umožnilo přepínat servery podle vytížení provozu, což vedlo k efektivnímu využívání vlastních kapacit [9].

Jedna z hlavních společností, která se zasloužila o rozšíření Cloud Computingu jak ho známe dnes, byla firma Salesforce.com. V roce 1999 představila koncept poskytování podnikových aplikací přes webové rozhraní. Po tom, co firma SalesForce úspěšně dokázala, že princip Cloud Computingu může fungovat i jinde než v oblasti telekomunikací, inspirovaly se i další velké společnosti. Firma Amazon, která využívala v tém době jen asi 10% své kapacity datových center, v roce 2002 vydala službu Amazon Web Service (AWS), která využívá principů Cloud Computingu a utilizovala nevyužívanou kapacitu zdrojů. Další čtyři roky poté spustila korporace Google služby Google Docs, což vedlo k významnému rozšíření povědomí o Cloud Computingu mezi veřejnost [10]. Tyto projekty se staly impulsem pro vznik velkého množství nových poskytovatelů cloudových služeb.

3.2 Cloud Computing podle NIST

Cloud Computing je v dokumentu [7] definován jako model služby, která umožňuje na vyžádání snadno dostupný síťový přístup ke sdíleným výpočetním zdrojům (např. sítě, servery, datová úložiště, aplikace a služby), které mohou být v případě potřeby rychle připraveny a dodány s minimálním usilím a interakcí poskytovatele.

NIST nabízí kromě samotné definice i základní principy a charakteristiky Cloud Computingu a vymezuje modely nasazení (Deployment Models) a distribuční modely (Service Models). Hlavním principům se bude věnovat další podkapitola 3.2.1 a modelům budou dále věnovány samostatné podkapitoly 3.2.2 a 3.2.3.

3.2.1 Charakteristiky

Definice Cloud Computingu podle NIST uvádí pět základních charakteristik [7].

Služby na vyžádání (On-demand self-service)

Uživateli je podle potřeby umožněn přístup k výpočetním kapacitám (server, síťová úložiště) automaticky, aniž by byla nutná interakce s poskytovatelem dané služby.

Širokopásmový přístup (Broad network access)

Uživateli je umožněn přístup k výpočetním kapacitám pomocí standardních mechanismů, které umožňují využití heterogenních tzv. tenkých nebo tlustých klientů (mobilní telefony, tablety, notebooky, stolní počítače, atd.).

Sdílení zdrojů (Resource pooling)

Výpočetní zdroje poskytovatele služeb jsou sdíleny mezi více uživatelů, avšak navzájem izolované. K tomu je využíván multi-tenant model, který tyto zdroje přerozděluje na základě poptávky uživatelů. Uživatel nemá kontrolu nad přesným umístěním sdílených prostředků, ale měl by být schopen určit jejich polohu na úrovni státu nebo datového

centra. Výpočetní zdroje zahrnují výpočetní výkon, paměť, datová úložiště, šířku pásma síťového připojení a virtuální stroje.

Rychlá flexibilita (Rapid flexibility)

Požadované služby jsou poskytovány rychle a poskytovatel zajišťuje elasticitu ve smyslu přidělování a odebírání požadovaných zdrojů v závislosti na jejich poptávce. Poskytované zdroje se uživateli jeví jako neomezené – jsou přidělovány v jakémkoliv množství a kdykoliv.

Měřitelnost služby (Measured Service)

Systémy automaticky řídí, kontrolují a monitorují využívání zdrojů, podávají transparentní informace na určité úrovni abstrakce odběrateli i poskytovateli (např. velikost úložiště, zpracování dat, šířka pásma, aktivní uživatelské účty). Uživatel má k dispozici celkové výdaje za poptávané služby a eliminuje tak náklady vynaložené na zjištění těchto informací.

Podle dokumentu od NIST, je nutné splnit všechny výše uvedené charakteristiky, abychom mohli mluvit o Cloud Computingu. V praxi tomu tak ale v mnoha případech není. Plně automatizovaný samoobslužný provoz mohou mít pouze největší poskytovatelé, vetšinou dodavatelé IaaS řešení.

3.2.2 Distribuční modely (Service Models)

Distribuční modely definují rozsah služeb, obvykle softwarových nebo hardwarových. Služby jsou uspořádány ve vrstvách, které ale na sobě mohou být částečně závislé, takže některé služby zasahují do více vrstev.

Dokument „The NIST Definition of Cloud Computing“ zavádí kategorizaci z hlediska typu a rozsahu poskytovaných služeb na tři distribuční modely: IaaS, PaaS, SaaS. Tyto modely jsou popsány v následujících podkapitolách.

V současné době se ale můžeme v literatuře setkat i s pojmem XaaS (X as a Service), kde X vyjadřuje libovolnou funkcionalitu dodávanou prostřednictvím internetu ve formě služby. Tento model v sobě zastřešuje tři hlavní modely IaaS, PaaS, SaaS a navíc zahrnuje i mnoho dalších variant a vycházejí z různých odvětví.

Software jako služba (Software as a Service, SaaS)

Zákazník používá aplikace poskytovatele, které běží na sdílené cloudové infrastruktuře [1]. Aplikace jsou přístupné prostřednictvím internetu z různých klientských zařízení, buď přes webový prohlížeč nebo programové rozhraní tenkého klienta. Uživatel služby neřídí a nespravuje infrastrukturu zahrnující sítě, servery, operační systémy, úložiště, ani individuální možnosti aplikace. Výjimkou mohou být specifická nastavení aplikace pro konkrétní uživatele [7]. Typickým příkladem SaaS jsou například Goodle Apps, Dropbox, OneDrive a jiné. V minulosti bylo využívání tohoto typu často považováno za bezpečnostní riziko. Většina provozovatelů se proto zaměřila na zvýšení bezpečnosti uživatelských dat, tím zatraktivnily své služby a jsou dnes masivně využívány širokou veřejností.

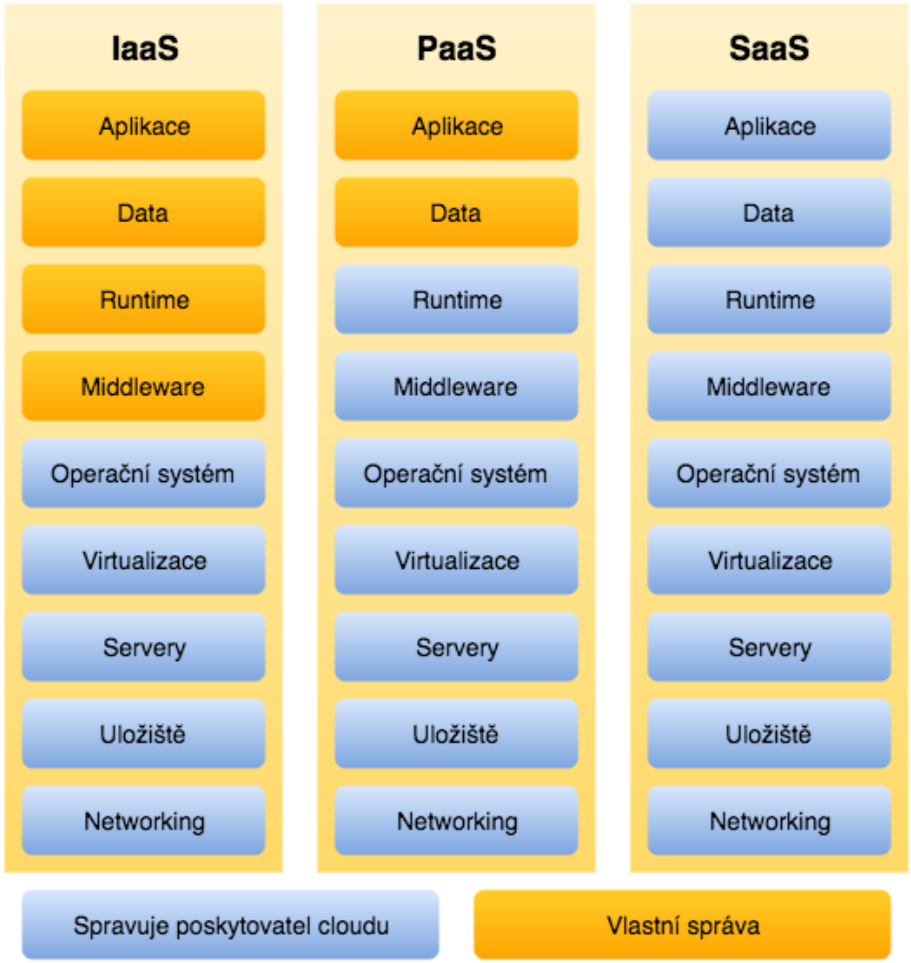
Platforma jako služba (Platform as a Service - PaaS)

Poskytovatel umožňuje uživateli provozovat v cloudu buď vlastní, nebo pronajaté aplikace. Takové aplikace jsou vytvořeny pomocí programovacích jazyků, knihoven, služeb a nástrojů podporovaných poskytovatelem, což ale nevylučuje použití kompatibilních programovacích jazyků, knihoven, služeb nebo nástrojů z jiných zdrojů. Jako u předchozího modelu uživatel nemá možnost spravovat cloudovou infrastrukturu, ale má kontrolu nad nasazením aplikací, správou vlastních aplikací a případnou konfigurací hostingu. Příkladem tohoto typu služby jsou Microsoft Azure, Google App Engine, AppScale nebo Red Hat OpenShift.

[1] Cloudová infrastruktura je kolekce hardwaru a softwaru, na kterou lze nahlížet jako na abstraktní a fyzickou vrstvu. Fyzická vrstva se skládá z hardwarových prostředků, které jsou nezbytné pro umožnění provozu poskytovaných cloudových služeb, typicky zahrnuje servery, úložiště, síťové prvky. Abstraktní vrstva se skládá ze softwaru nad fyzickou vrstvou. [7]

Infrastruktura jako služba (Infrastructure as a Service - IaaS)

Poskytovatel zajišťuje uživateli výpočetní výkon, datová úložiště, sítě a další základní výpočetní zdroje. Ty má uživatel k dispozici pro nasazení a používaní libovolného softwaru, který zahrnuje provoz systémů a aplikací. Opět zde platí, stejně jako u modelů Saas a PaaS, že uživatel není schopen řídit nebo kontrolovat základní cloudovou infrastrukturu, ale má kontrolu nad operačními systémy, ukládáním a správou aplikací a případnou omezenou kontrolu vybraných síťových prvků (např. hostitelské firewally) [10]. Mezi hlavní technologie této služby patří virtualizace hardwaru, kde jeden i více serverů může být spojeno podle potřeb v distribuovaný systém, na kterém jsou potom aplikace instalovány a spouštěny.



Obrázek 3.1: Rozdělení modelů Iaas, Paas, SaaS podle správy služeb, vlastní zpracování

3.2.3 Modely nasazení (Deployment Models)

Cloudové služby jsou dále děleny také podle způsoby implementace. Dokument „The NIST Definition of Cloud Computing“ [7] zavádí následující čtyři modely.

Privátní cloud (Private cloud)

Infrastruktura privátního cloudu funguje výhradně pro účely konkrétní organizace zahrnující skupinu uživatelů. Může být vlastněna a spravována přímo organizací nebo třetí stranou. Pokud organizace využívá vlastní datové centrum, pak se používá označení on-site private cloud. Pokud organizace využívá naopak datové centrum poskytovatele, který se stará navíc o jeho údržbu, tak se jedná o outsourced private cloud.

Motivací organizace pro vytvoření on-site private cloudu je efektivní využití firemního hardware a možnost nabízet software ve formě služby svým zaměstnancům, dodavatelům i zákazníkům.

Outsourcovaný privátní cloud si organizace pronajímá a jeho prostor je fyzicky oddělen v datovém centru poskytovatele od ostatních odběratelů. Přínos pro organizaci využívající outsourcovaný cloud je v úspoře na nákladech spojených s nákupem a údržbou hardware.

Komunitní cloud (Community cloud)

Principem komunitního cloudu je sdílení infrastruktury cloudu mezi několik organizací se stejnými zájmy. Podobně jako u privátního cloudu může být cloud umístěn v rámci organizace nebo hostovaný.

Veřejný cloud (Public cloud)

Jedná se o model veřejného cloudu, který je k dispozici široké veřejnosti nebo velké průmyslové skupině. Cloudová infrastruktura je umístěna u poskytovatele. Jde o nejběžnější typ cloudu, který se vyskytuje.

Hybridní cloud (Hybrid cloud)

Hybridní cloud spojuje dva a více typů cloudu (privátní, komunitní, veřejný). Jednotlivé typy cloudu přitom zůstávají samostatné, ale jsou spojeny standardizovanou technologií, která umožňuje přenos dat a aplikací.

3.3 Výhody a nevýhody

Tato kapitola shrnuje hlavní výhody a nevýhody cloudových řešení, vychází především z publikací [7], [11] a [12].

3.3.1 Výhody

Dostupnost

Uživatel může k datům přistupovat odkudkoliv, nezávisle na aktuálně používané platformě.

Rychlost

Cloudová řešení přinášejí koncepci centralizované platformy, která je kdykoliv připravena k rychlému použití, údržba infrastruktury je prováděna automaticky a opravy jsou řešeny v krátkém časovém horizontu.

Flexibilita

Přístupové zdroje mají virtuální charakter, takže výsledný potenciál cloudu není limitován výkonností a kapacitou lokálních nebo vzdálených počítačů.

Efektivní sdílení prostředků

Sdílené hardwarové prostředky umožňují lépe distribuovat výkon mezi jednotlivé uživatele, efektivní přidělování zdrojů eliminuje i plýtvání elektrické energie.

Eliminace nákladů na správu a údržbu

Využití cloudu eliminuje podstatnou část aktiv spojených s údržbou jako je projektování, výběr softwarových a harwarových platforem, prostorů i personálu.

Nižší náklady

Outsourcované cloudové služby znamenají nižší finanční náklady, některé cloudové služby jsou dokonce poskytovány zcela zdarma nebo bezplatně v omezeném čase nebo rozsahu.

3.3.2 Nevýhody

Závislost na poskytovateli

Tato nevýhoda souvisí s jednou z hlavních výhod. Poskytovatel zajišťuje sice veškeré opravy a aktualizace, zároveň ale může kdykoliv své hostované služby změnit nebo ukončit, bez ohledu na zákazníka [12]. Zákazník využívající cloud dále ztrácí možnost rozhodovat, který software a verzi využívat. Je nutno počítat i s možností, že poskytovatel významně změní podmínky poskytování služeb tykajících se cen změnou kapacity. Je vhodné vybrat takového poskytovatele, kde toto riziko hrozí co možná nejméně.

Nedůvěra

Vzhledem k tomu, že cloud computing ve firmách je relativně nová záležitost. Neexistují zatím spolehlivá doporučení ohledně používání cloudu. Samotné využívání dat přes internet s sebou přináší mnohá bezpečnostní rizika. Smlouvy poskytovatelů často zahrnují varování, že poskytovatel nenese zodpovědnost za ztrátu dat uložených v cloudu, dokonce si některé organizace vyhrazují právo s nimi zacházet jako s vlastními, případně je odevzdat třetím stranám, například při vyšetřování zločinu. Nicméně je v jejich zájmu, aby k těmto případům docházelo co nejméně, jen v případě výjimečných situací, aby neztratili důvěru zákazníků.

Méně funkcí a komfortu v uživatelském rozhraní

Cloudová řešení většinou poskytují méně funkcí v porovnání s desktopovými aplikacemi. Podnik dokonce může mít tak specifické potřeby, které zatím nejsou pokryty levnějším cloudovým řešením.

Menší stabilita

Protože jde o přístup k datům prostřednictvím internetu, je velká míra stability závislá na stabilitě internetového připojení. Služby, ke kterým přistupujeme online mohou občas fungovat pomaleji nebo být dokonce nějakou dobu nedostupné, a to v případě, kdy konektivita selže úplně.

Legislativní problémy

Tato rizika souvisí hlavně s fyzickým uložením dat na serveru poskytovatele. Poskytovatelé a uživatelé sídlí v různých zemích s různými právními normami a jinými zákony týkajících se ochrany osobních údajů. Proto ne všechny údaje jsou vhodné pro ukládání v centralizovaných datových centrech.

Bezpečnostní problémy

Bezpečnost dat je jedním z nejdůležitějším aspektů, které je třeba v rámci cloudového řešení zajistit. Zde je zmíněno několik hlavních hrozeb v souvislosti se zabezpečením cloudu.

Výpadky Pokud jsou data uložená na serverech, je třeba se věnovat rizikům spojených se ztrátou výkonu nebo výpadku díky neočekávané vysoké zátěži. Dnešní řešení cloudových úložišť dokáže těmto problémům předcházet. Lze pružně a dynamicky přizpůsobovat alokované zdroje takovým způsobem, aby nedocházelo k přetížení.

Utajení Pokud podnik nevyužívá vlastního datového centra a vlastních systémů, je vhodné zajistit bezpečnost dat šifrováním.

Ztráta a odcizení hardware Prostřednictvím Cloud Computingu lze řešit problémy se ztrátou dat. V běžném podnikovém prostředí existuje riziko, kdy zaměstnanci si nahrávají důvěrná nebo kritická data na svá osobní zařízení nebo USB disky. Pokud jsou tato zařízení ztracena nebo odcizena může vzniknout podniku značná škoda. Centralizovaným uložením dat lze tato rizika eliminovat.

Aktualizace Dalším rizikem jsou chyby v softwaru, které mohou dát za vznik nedostatkům z hlediska bezpečnosti. Pokud podnik využívá vlastní software, je nutné, aby se o něho pravidelně staral, prováděl aktualizace. Ne však v každém podniku je pro tyto činnosti vyhrazen dostatek času a pracovníků. Využití Cloud Computingu přináší výhodu v tom, že za aktualizace odpovídá poskytovatel cloudového řešení, a tím je zajištěna vyšší stabilita a spolehlivost systému. S aktualizacemi softwaru souvisí i problém s viry. V běžném firemním IT prostředí se zpravidla sice využívá antivirových programů, nicméně v důsledku například nízkého výpočetního výkonu nebo nedostatečně aktualizovaným virovým skenerům je rozpoznání škodlivého softwaru obtížné. U Cloud Computingu toto zajišťuje opět poskytovatel, který se stará o automatické aktualizace antivirové ochrany.

Zabezpečení před útoky Určitě neopomenutelným problémem jsou útoky hackerů, o kterých je slyšet stále častěji, a proto je třeba jim věnovat nemalou pozornost. Útoky mohou teoreticky přijít z jakéhokoliv prostředí. V klasické firemní IT infrastruktuře nese podnik zodpovědnost za ochranu sám a musí tak zajistit patřičná opatření jako jsou například Firewall, Intrusion Detector, skenování virů atd. Při delegování služeb na cloudového poskytovatele je v rozsahu těchto služeb od zmíněných opatření osvobozen, protože v tomto případě za bezpečnost nese zodpovědnost opět poskytovatel.

Hijacking Jedná se druh útoku, kdy neoprávněná osoba získá přístup do podnikového systému. K přístupu využívá nelegálně získaných přístupových údajů oprávněných uživatelů. Jednou ze známých technik získávání citlivých údajů je phishing, kdy je uživatel nabádán prostřednictvím internetu k vyplnění svých přihlašovacích nebo jinak citlivých údajů, které jsou následně zneužity. Prostředkem phishingu je na-

příklad často komunikace přes emailové zprávy, která předstírá, že pochází od důvěryhodných zdrojů například poskytovatele softwaru, IT administrátora apod. [13] V souvislosti s cloud computingem se nejčastěji hovoří o útoku na účet nebo službu. Nejrizikovějším faktorem hijackingu ve firmě jsou zaměstnanci. Především by neměli používat příliš jednoduchá hesla nebo hesla stejná, které využívají k jiným účtům. Dále by se neměly v žádném případě přihlašovací údaje přeposílat mezi jednotlivými uživateli. Ochranou proti tomuto riziku je hlavně dobrá informovanost zaměstnanců.

Malicious insiders Jde o útoky, které přichází zevnitř podniku. Rizikem jsou zaměstnanci nebo obchodní partneři s přístupem do podnikové sítě, kteří úmyslně zneužijí své pravomoci a negativně tím ovlivní důvěryhodnost, celistvost nebo dostupnost dat v systému [14].

4 Analýza současného stavu

Podstatou této práce je najít vhodné řešení pro podnik, který zvažuje nasazení nového systému pro ukládání, sdílení a synchronizaci podnikových dat. Motivací je snaha mít všechna podniková data uložena fyzicky ve firmě na vlastním serveru a také zlepšení kolaborativní práce zaměstnanců na projektech.

V této kapitole se zaměřuji na současný stav podniku a požadavky na nový systém. První podkapitola 4.1 obsahuje představení podniku. V další podkapitole 4.2 je vypracována studie příležitosti projektu nasazení nového systému a poslední podkapitola 4.3 se zabývá zjištěnými požadavky na hledaný systém.

4.1 Představení podniku

Cílová firma se zabývá vývojem mobilních aplikací pro děti předškolního věku. Misí této firmy je poskytovat kvalitní a efektivní vzdělání prostřednictvím speciálně navrženého výukového portfolia herních aplikací. Společnost do loňského roku primárně vyvíjela pro mobilní platformu iOS, tedy systémy využívající zařízení značky Apple. Loni svoje produkty rozšířila na platformu Android a Windows Phone. Cílem firmy je do roku 2021 připravit komplexní vzdělávací systém, který bude schopen z velké části pokrýt požadavky na vzdělání dětí předškolního věku.

Další informace jsou obsaženy v kapitole 4.2 v rámci zpracovaných analýz o tomto podniku.

4.2 Studie příležitosti projektu

Obsahem studie příležitosti jsou analýza obecného okolí podniku, dále analýza oborového okolí podniku a analýza interního prostředí firmy, které můžeme najít v sekcích 4.2.1, 4.2.2 a 4.2.3. Zhodnocení situace firmy v podkapitole 4.2.4 je vyjádřeno prostřednictvím metody SWOT a navazuje na něho celkové vyhodnocení studie v podkapitole 4.2.5.

4.2.1 Analýza obecného okolí metodou SLEPT

Sociální faktory

Podnik se zejména v poslední době značně rozrůstá, proto nabízí mnoho pracovních příležitostí. Většina zaměstnanců pracuje v pražské pobočce, zároveň má firma i 20 externích zaměstnanců. V tomto roce byla nově otevřena pobočka v San Franciscu, kde se v současné době tvoří tým pracovníků.

Počet dětí, které se již v předškolním věku prostřednictvím zařízení svých rodičů dostávají k mobilním aplikacím, roste. Mobilní hry a aplikace se tak v současnosti stávají silným výukovým nástrojem. Vzhledem k tomu, že celosvětová porodnost má rostoucí trend a zároveň stále více lidí vlastní chytré mobilní telefony nebo tablety, společnost se nemusí obávat snížení počtu cílových uživatelů.

Legislativní faktory

Všechny aplikace jsou nabízeny zákazníkům přes AppStore (aplikační market pro zařízení s operačním systémem iOS) a Google Play Store (aplikační market pro zařízení s operačním systémem Android). Do současné doby není obsah mobilních her významně omezován či kontrolován. Firma ale u většiny svých produktů při vydání žádá také o zařazení do seznamu doporučených aplikací ve zmiňovaných aplikačních marketech. V tomto případě např. firma Apple přísně kontroluje obsah her vzhledem k věku cílových uživatelů, což může vést ke zpoždění vydání některých her a ohrozit i například úspěšnost reklamní kampaně, pokud produkt nebude na trh uveden včas.

Ekonomické faktory

Aplikace čelí velkému počtu konkurenčních produktů, které jsou dostupné zdarma. Obchody, které nabízejí mobilní aplikace si nárokují značnou část z prodejní ceny a také mohou definovat minimální výši ceny aplikace (v případě, že se nejedná o zcela bezplatnou). Stanovené ceny se zatím nemění ani v reakci na změnu měnového kurzu.

V loňském roce společnost koupila mateřskou školu a otevřela pobočku v San Franciscu, a tak se v krátké budoucnosti neplánují další větší investice.

Politické faktory

Společnost je závislá na politice pouze jako na orgánu měnícím legislativu a daňové sazby.

Technologické faktory

Podnik v současné době využívá k vývoji aplikací herní framework, který je dostupný zdarma a je pravidelně aktualizován. Zároveň ale zodpovědné osoby sledují výzkum technologií a v případě uvedení na trh vhodnější technologie, může podnik zvážit přechod na novou technologii.

Konkurenční výhodu představuje vlastní nástroj na vykreslení grafických prvků v aplikacích, který umožňuje efektivní používání animací. Do budoucna je v plánu tento produkt prodávat samostatně.

Mobilní aplikace jsou testovány pouze na vybraném vzorku mobilních zařízení, je tedy možné, že na některých zařízeních nemusí být funkcionalita úplná. Zatímco zařízení s operačním systémem iOS existuje jen několik typů, tak systém Android do svých telefonů instaluje velké množství výrobců a není tak možné otestovat hry na každém z nich. Podobně je to i s funkcionalitou s ohledem na verzi operačního systému. Podnik se snaží zajistit funkcionalitu hlavně u aktuálních verzí, ale zejména u dlouho neaktualizovaných systémů může dojít k chybovosti aplikace.

Ke sdílení dat mezi odděleními v podniku firma od počátku využívá úložiště Google Drive a online systém na tvorbu a úpravu dokumentů Google Docs. Jako komunikační kanály jsou využívány emailová a chatová komunikace také od firmy Google. Vzhledem

k růstu počtu zaměstnanců ve firmě začíná být uspořádání dat a uživatelů nepřehledné. Chybí správné rozdělení zaměstnanců dle oddělení a přiřazení přístupových práv k prohlížení dokumentů. Data jsou uložena na servech firmy Google, což není z hlediska bezpečnosti vhodné řešení.

4.2.2 Analýza oborového okolí pomocí Porterova modelu

Rivalita s konkurencí

V rámci České republiky na trhu téměř neexistuje konkurence, která by nabízela podobnou kolekci her zaměřených na předškolní děti. V celosvětovém měřítku existují podobně zaměřené podniky, například švédská firma Toca Boca nebo Sago Sago z Kanady. Společnosti mezi sebou soutěží a snaží se své produkty lokalizovat do světových jazyků a opatřit aplikace certifikáty, které ručí za kvalitu vzdělávací složky her. Certifikáty a ocenění přinášejí podnikům konkurenční výhodu na trhu.

Hrozba vstupu nových konkurentů

Vzhledem k trvale stoupajícímu trendu poptávky po produktech a nenasycenosti trhu je téměř jisté, že počet nových konkurentů se bude zvyšovat. Vstup na tento trh je poměrně jednoduchý a počáteční investice není nijak velká. Avšak pro tak komplexní řešení, jako v současné době podnik má, je třeba i větší vstupní kapitál.

Vyjednávací síla zákazníků

Produkty jsou nabízeny za pevné ceny uvedené na internetových obchodech k tomu určených. V rámci dočasných akcí jsou hry nabízeny za zvýhodněnou cenu nebo ve formě zvýhodněných cenových balíčků. Kromě běžného prodeje prostřednictvím aplikačních marketů AppStore nebo Google Play Store také firma nabízí své portfolium her mateřským školám a vzdělávacím centrům pro předškolní děti.

Vyjednávací síla dodavatelů

Podnik nemá žádného přímého dodavatele.

Hrozba substitutů

V současné době je na trhu v celosvětovém měřítku mnoho firem, které se zaměřují na dětské mobilní aplikace v různých grafických provedeních, zvukových kvalitách a jazykových možnostech. Hrozba substitutů je tedy vysoká. Podniků, které konkurují jednotlivým produktům je velké množství, ale jak bylo zmíněno výše, většinou se nejedná o tak komplexní řešení lokalizované do více světových jazyků. Výskyt substitutů má ale významný vliv na cenu produktu.

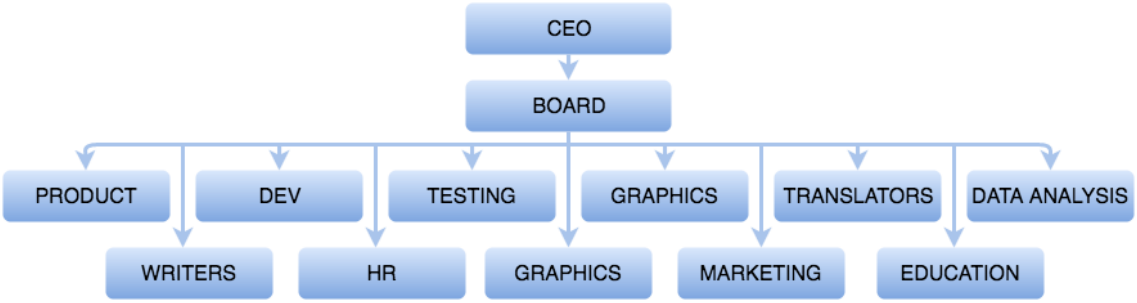
4.2.3 Analýza interních faktorů metodou „7S faktorů“

Strategie

Jelikož je firma menším podnikem, neexistuje žádný dokument, který by strategii blíže popisoval. Strategie je tak pouze ve vizích majitele. Dlouhodobý záměr firmy je však vytvoření komplexního vzdělávacího systému pro děti předškolního věku, získání nových zákazníků, zvýšení počtu stažení vydaných aplikací a zvyšování hodnoty podniku. Jako dílčí strategické cíle v nadcházejícím období si firma stanovila rozšíření lokalizací až do 20 jazyků a rozšíření portfolia produktů o aplikace pro interaktivní četbu.

Struktura

Firma je organizována na bázi vedoucí rady a k ní podřízených manažerů jednotlivých oddělení. Firma nemá vlastní IT oddělení ani personální oddělení, ale využívá služeb mateřské společnosti. Celkový počet zaměstnanců je 60, z nichž asi třetina pracuje externě, zejména jde o překladatele z různých částí světa.



Obrázek 4.1: Organizační struktura podniku

Systémy

Vzhledem k velkému počtu oddělení, rostoucímu počtu zaměstnanců i externím pracovníkům je klíčový efektivní systém komunikace a práce na sdílených datech. Data a zdroje k projektům jsou uložena na firemním serveru, ale jsou využívána hlavně vývojovým a grafickým oddělením. K verzování projektů se využívá systém Git. Jak bylo zmíněno výše, při komunikaci a při práci na sdílených dokumentech zaměstnanci firmy zatím používají prvotně zavedený systém od firmy Google. Problémem je, že v posledních měsících se firma značně rozrostla a dosavadní komunikační kanály přestávají být dostačující. Struktura dokumentů přestává být přehledná a největším nedostatkem je, že se data fyzicky nacházejí mimo podnik v datovém centru poskytovatelské společnosti Google.

Styl řízení

Styl řízení ve firmě je demokratický. Většina rozhodování o firemních záležitostech jsou sice primárně na jednateli společnosti, který se ale radí s celou vedoucí radou. Některé druhy rozhodnutí jsou delegovány na vedoucí jednotlivých oddělení. Pravidelně se také pořádají schůze středního managementu, kde se řeší návrhy na nové i probíhajících projekty. Každý zaměstnanec má možnost prostřednictvím vedoucího svého oddělení sdělit své připomínky k řízení. Při rozhodování o podobě nově vznikajících produktů se pořádají diskuze, kde se může zapojit každý zaměstnanec.

Sdílené hodnoty

Vztahy ve firmě jsou přátelské až rodinné, což podporuje motivaci zaměstnanců a ochotu spolupracovat. Zaměstnanci mají možnost podílet se na návrhu produktů, jejich podobě a je vítána jakákoliv zpětná vazba k již vydaným produktům. Zároveň podnik umožňuje zaměstnancům účastnit se konferencí, speciálních událostí za účelem firemní prezentace nebo testovacích dnů v mateřských školách.

Spolupracovníci

Pro společnost je důležité motivovat své zaměstnance a vytvářet přívětivé pracovní prostředí, aby zůstali své firmě věrní. Zaměstnanci jsou motivováni bonusovým finančním ohodnocením, které se uděluje formou variabilní částky ve výši, která je stanovena každý měsíc s ohledem na pracovní výkony konkrétního zaměstnance. Pracovníkům je umožněno účastnit se porad a přispívat do diskuze týkající se dalšího chodu firmy.

Schopnost

Zaměření pracovníků odpovídá jejich činnostem v rámci podniku, nicméně během několika měsíců dochází k odhalení jejich dalších schopností a stává se, že zaměstnanci migrují mezi odděleními. Firma umožňuje zaměstnancům jejich schopnosti a dovednosti uplatnit a zdokonalovat, jak v náplni jejich práce, tak mimo ni. V rámci své pracovní doby se mohou pracovníci účastnit i kurzu anglického jazyka, který je dotován zaměstnavatelem. Podnik také umožňuje svým zaměstnancům účastnit se mezinárodních konferencích zaměřených na vývoj her, počítačových technologií, vzdělávání apod. V oboru informačních technologií je zvyšování schopností a dovedností velice důležitým faktorem, aby firma nezůstala pozadu za konkurencí.

4.2.4 SWOT analýza

Následující SWOT analýza navazuje na informace získané pomocí předchozích analýz.

Silné stránky (Strengths)	**Slabé stránky** (Weaknesses)
• vlastní zdroje financování • vlastní grafický software • produkty dostupné v devíti světových jazycích • kvalifikovaný personál	• nedostatečně strukturovaný informační systém • pomalé komunikační procesy • ukládání citlivých podnikových dat na cizí server
Příležitosti (Opportunities)	**Hrozby** (Threats)
• rostoucí poptávka po vzdělávacích aplikací pro děti • lokalizace do 15 světových jazyků • nabízet grafický software jako samostatný produkt	• omezení a kontroly ze strany internetových obchodů • zpoždění příchodu na trh s novými produkty • rychle rostoucí konkurence • rychle měnící se technologie

Tabulka 4.1: SWOT analýza společnosti, vlastní zpracování

4.2.5 Vyhodnocení

Na základě vypracovaných analýz bylo zjištěno, že změna systému je jednoznačně jednou z vhodných změn, která by měla vést ke zvýšení konkurenceschopnosti podniku a zlepšení pracovních procesů a efektivity práce zaměstnanců. Na základě výsledků studie příležitosti lze navrhovaný projekt označit jako vhodný pro firmu s přihlédnutím na její současný i očekávaný budoucí stav.

4.3 Požadavky na systém

Firma představila požadavky, které by mělo výsledné řešení ukládání podnikových dat splňovat v co největší míře:

Bezpečnost dat Důležitý požadavek má společnost na zabezpečení dat. Všechna data včetně záloh si chce firma uchovávat fyzicky v prostorách firmy a neposkytovat tato data pod správu jiným firmám. Pro tyto účely má již firma ve svém majetku server, který je vhodné využít.

Kalendář Dalším požadavkem je řešení pro tvorbu a sdílení kalendářů mezi zaměstnanci, v ideálním případě rozdělených podle oddělení ve firmě.

Dokumenty Nový systém by měl obsahovat nástroj, který poskytne řešení pro kolaborativní práci zaměstnanců na textových souborech. Výsledkem by měla být možnost efektivně tvořit dokumenty například pro popis vznikajících produktů nebo reklamních kampaní.

To-do listy Hledané řešení by mělo přinést možnost správy osobních to-do listů. Výhodou by byla možnost sdílení takových seznamů mezi zaměstnanci.

All-in-one řešení Podnik preferuje jedno komplexní řešení před systémem složených z dílčích nástrojů, které by bylo třeba spravovat zvlášť.

Multiplatformnost Důležitým požadavkem je multiplatformnost, protože zaměstnanci firmy používají všechny tři hlavní platformy (Linux, Windows, Mac OS X).

Cena Firma hledá takové řešení, u kterého by nemusela platit pravidelné licenční poplatky nebo které by vyžadovalo větší investici na jeho nákup.

Open source Protože se zároveň jedná o podnik zabývající se informačními technologiemi a firma má mezi zaměstnanci početnou skupinu programátorů, je vhodné zaměřit se na open source nástroje. V případě, že by nějaká z požadovaných funkcionalit chyběla, firma si ji může sama doimplementovat.

Technická podpora Nástroj by měl mít funkční podporu a možnost nahlašování případných chyb.

5 Vlastní návrh řešení

Tato kapitola se zabývá samotným návrhem řešení. V první podkapitole 5.1 jsou analyzovány požadavky a je vybrána nejvhodnější technologie. V další podkapitole 5.2 jsou detailněji popsány vlastnosti zvoleného řešení, je popsán postup nasazení v podniku a konfigurace systému pro potřeby dané společnosti. Třetí podkapitola 5.3 obsahuje rizikovou analýzu vybraného řešení.

5.1 Výběr technologie

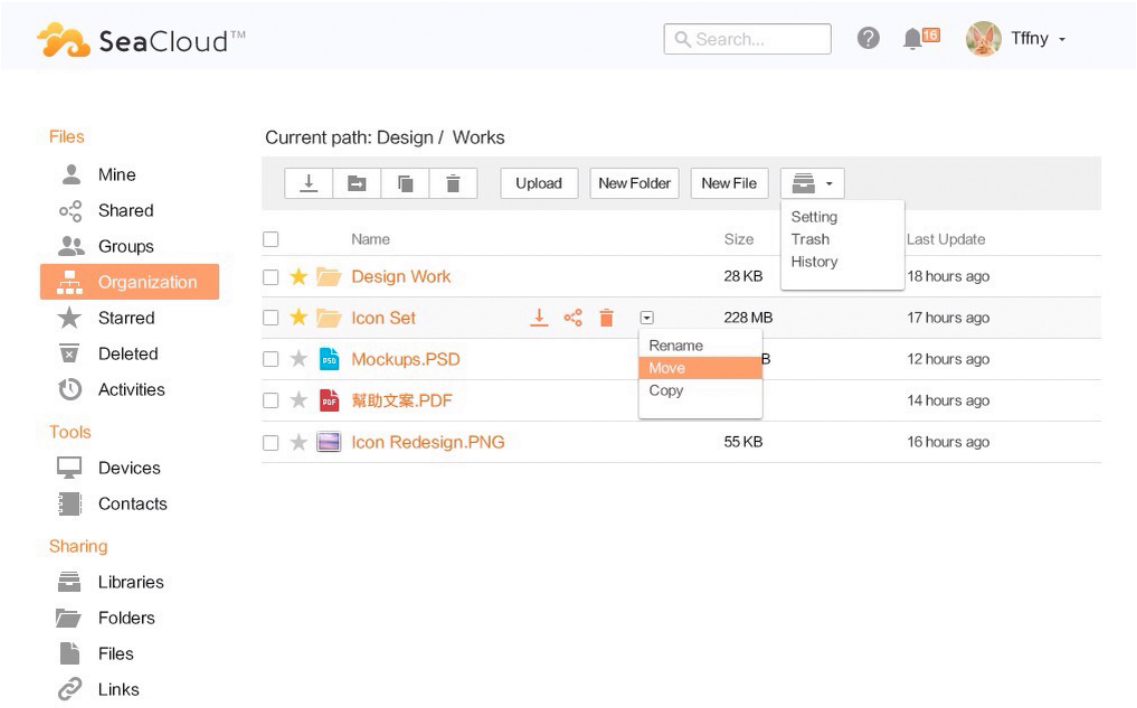
Požadavky podniku jsem roztřídila a určila ty klíčové, které velmi zužují možný výběr nástrojů. Mezi takové požadavky patří například body ohledně open source řešení a bezpečnosti dat. Protože si firma nepřeje, aby byla data fyzicky umístěná mimo firmu, je zřejmé, že hledaným řešením je privátní cloud nasazený na vlastním serveru. V tomto případě musíme vyloučit řešení typu DropBox nebo Google Apps. Tato řešení také vylučuje požadavek firmy na bezplatné řešení.

Dalším podstatným bodem je požadavek na multiplatformnost. Při řešení je třeba brát ohled na to, zda systém nabízí klientské programy pro všechny nejrozšířenější platformy. Jelikož se očekává, že nástroj budou používat všichni zaměstnanci a dlouhodobě, tak bod o možnosti nahlašování chyb nám vyřazuje z výběru nástroje, které mají vývoj už zastavený nebo neumožňují nahlašování chyb. Do užšího výběru jsme zvolili 3 aktuálně nejznámější nástroje a to Seafile, Synthink a ownCloud.

5.1.1 Seafile

Synchronizační nástroj Seafile se vyznačuje svojí stabilitou. Uživatelé si chválí hlavně bezproblémový přechod mezi verzemi a spolehlivost přenosu dat. Z hlediska využití ve zmiňovaném podniku je jeho hlavní nevýhodou, že řeší pouze synchronizaci dat. Ostatní služby, které podnik požaduje, jako je sdílený kalendář nebo kolaborativní práce na souborech, by musely zajišťovat další samostatné nástroje.

Velkou výhodou Seafile je jeho rychlost. Serverová část je napsána majoritně v jazyce C. Podporuje správu uživatelů přes Active Directory nebo LDAP. Vývojáři Seafile kladli velký důraz i na bezpečnost, a tak šifrování ukládaných souborů je přímo vestavěné do hlavní části nástroje. Na obrázku 5.1 je náhled uživatelského rozhraní systému Seafile.



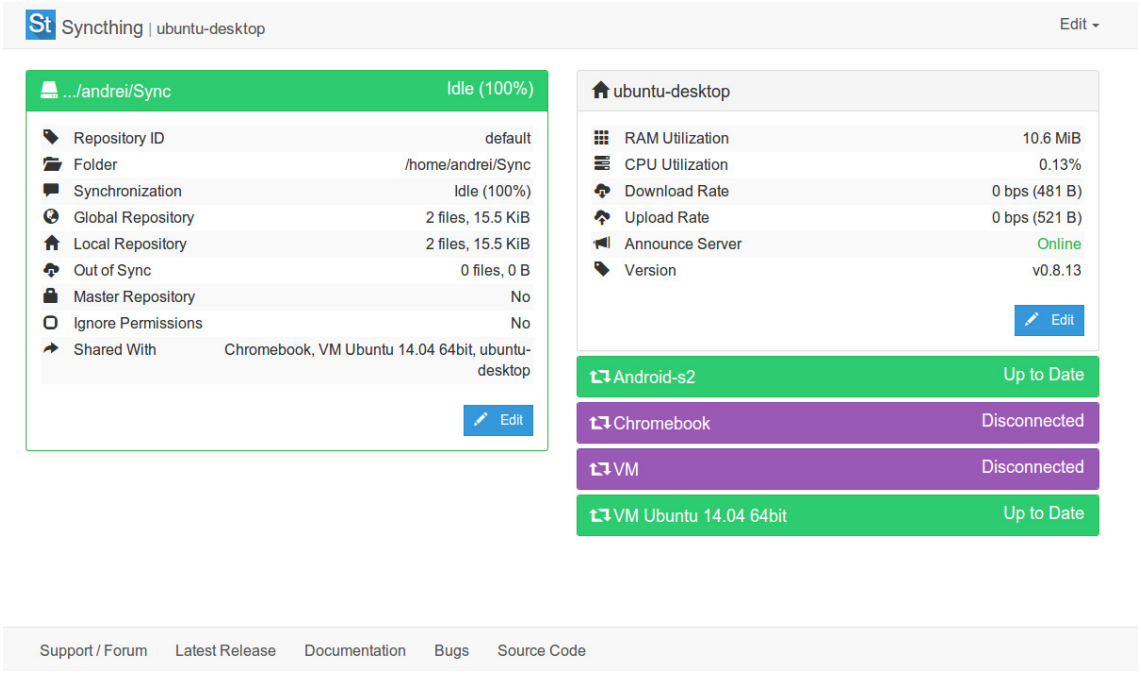
Obrázek 5.1: Náhled na hlavní webové rozhraní Seafile

5.1.2 Syncthing

Syncthing je nejnovější z porovnávaných nástrojů. Jeho vývojáři se zaměřili hlavně na přenositelnost, rychlost a bezpečnost dat.

Zdrojový kód nástroje Syncthink je napsaný v jazyce Go, což umožňuje systémový program zkompilovat a používat na jakékoliv platformě. Z porovnaných nástrojů je určitě Syncthink ten nejrychlejší. Rychlost systému je nespornou výhodou, protože ve firmě je třeba synchronizovat velké množství binárních dat aplikací. Důvodem lepší rychlosti systému je rozhodnutí vývojářů navrhnout a implementovat vlastní protokol a nespoléhat se na existující protokoly, které přinášejí řadu omezení.

Hlavní nevýhodou nástroje je, podobně jako u nástroje Seafile, že s ním lze řešit pouze synchronizaci souborů. Tím ale seznam nevýhod nekončí. Synthink sice disponuje webovým rozhraním, ale toto rozhraní slouží jen na párování zařízení a nastavení sdílení dat. Přes webové rozhraní není možné prohlížet jednotlivé soubory. Dále nelze při synchronizaci vybrat jen určité podsložky, vždy se synchronizuje celý obsah. Správa uživatelů je sice možná, ale administrace je velmi těžkopádná a zcela chybí podpora rozdělení uživatelů do skupin.



Obrázek 5.2: Náhled na hlavní webové rozhraní Syncthink

5.1.3 Owncloud

OwnCloud je velmi rozšířené řešení primárně určené na synchronizaci souborů, ale taktéž pro sdílení kalendářů, to-do listů, kolaborativní práci na dokumentech a disponuje množstvím rozšíření, která zabezpečují další funkcionalitu.

Je možné ho nasadit na Linux nebo Windows server. Je napsaný v jazyce PHP a kvůli tomu je synchronizace pomalejší. Aktuálně je ale rychlost jedna z hlavních priorit vývojového týmu. OwnCloud je oblíbený nástroj v open source komunitě, takže disponuje velkým počtem vývojářů, a proto jde jeho vývoj rychle vpřed a chyby se častokrát odstraňují velmi rychle po jejich nahlášení.

OwnCloud nabízí klientům širokou nabídku produktů, ať už se jedná o synchronizační klienty na Windows, Linux nebo Mac OS X, nebo o mobilní aplikace na vysoké úrovni, z nichž je většina nabízena bezplatně.

Nasazení OwnCloudu je poměrně jednoduché, dokonce mnohé z Linuxových distribucí (Debian, CentOS) obsahují již předpřipravené balíky, které stačí nainstalovat a ownCloud v základním nastavení je připraven k provozu.

Mezi hlavní nevýhody ownCloudu patří jeho známé problémy při přechodu na novější verze. Update ownCloudu může vést k problémům na serveru a je potřeba zkušeného administrátora, který dokáže dát všechno do pořádku.

Velkou výhodou ownCloudu je ale jeho velmi propracována práce se soubory, možnost ukládání revizí, sdílení souborů a složek s jinými uživateli ownCloudu nebo možnost sdílení pomocí URL odkazů, které je možné zaslat třetím osobám.

5.1.4 Zhodnocení

Do užšího výběru k porovnání jsem vybrala nástroje Synthing, Seafile a ownCloud. Každý z těchto nástrojů má jiné přednosti a také nevýhody. Seafile je známý svojí stabilitou a bezproblémovým přechodem na nové verze, což zároveň patří mezi největší nevýhody řešení ownCloud, který právě s updatem na novější verze má velké problémy. Synthing má zase velmi propracovaný synchronizační protokol, který se vyznačuje svojí rychlostí

a bezpečností. Bohužel oproti Seafile a ownCloudu slouží jen na synchronizaci souborů a nemá ani zdaleka tak rozšířenou funkcionalitu.

Seafile a ownCloud jsou podobná řešení a obě z velké části splňují požadavky na hledaný software. Nakonec jsem se rozhodla pro ownCloud a to z více důvodů. Jedním z hlavních důvodů je jeho komunita a probíhající rychlý a silný vývoj. Právě díky komunitě disponuje rozsáhlými možnostmi ohledně rozšíření. Do budoucna se předpokládá, že budou přibývat další nové funkcionality. Dalším důvodem volby ownCloudu je programovací jazyk, v kterém je napsán. Oba nástroje jsou open source, což znamená, že firma si v případě potřeb může funckionalitu sama rozšířit podle svých potřeb. Seafile je z velké části napsaný v jazyce C, jeho pochopení a rozšiřování by zabralo více času, než je tomu v případě ownCloudu napsaného v jazyce PHP.

5.2 Cloudové řešení ownCloud

Tato kapitola se zabývá podrobněji vybraným řešením, představuje obecné možnosti zvoleného systému i vlastnosti související s požadavky konkrétního podniku.

5.2.1 Bezpečnost dat

Citlivým tématem dnešní doby je bezpečnost a o kauzách souvisejících s únikem dat slýcháme stále častěji. Se službou ownCloud bude moci podnik přesně sledovat, kde se jeho data fyzicky nacházejí a je možné šifrovat je přímo na serveru. To znamená, že i v případě, že by byl podnikový server kompromitován, budou pro útočníka data nečitelná.

Stejně tak komunikace mezi ownCloud serverem a klientskými zařízeními může být šifrovaná firemním certifikátem, u kterého je možné si dle vlastního uvážení nastavit úroveň zabezpečení.

Nespornou výhodou ownCloudu je otevřený kód, kde je možné se ujistit, že vývojáři si úmyslně nevytvořili možnost pro zneužití dat. Navíc existující komunita kolem ownCloudu se mimo jiné zabývá právě hlídáním kódu z hlediska jeho bezpečnosti.

K ownCloudu lze připojit i jiné úložiště, například Google Drive nebo Dropbox. Zabezpečení lze zajistit tak, že data budou připojena přes vlastní firewall, který bude filtrovat případné podezřelé soubory.

5.2.2 Spolehlivost

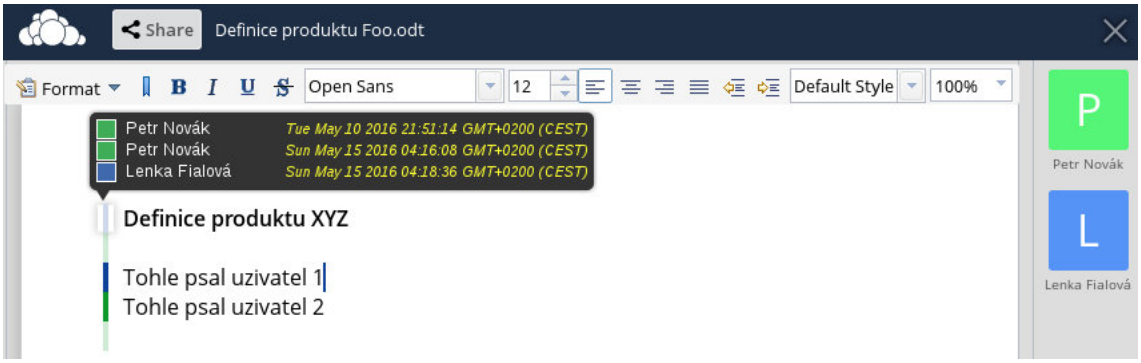
Spolehlivost závisí na zařízení, na kterém je ownCloud nasazen. Dosažení maximální dostupnosti by bylo možné využitím clusterů více fyzických serverů a v případě výpadku mezi nimi přepínat.

Na firemní serveru, který by byl vhodný pro nasazení ownCloudu, je nainstalován databázový server MariaDB. Ten má přímou podporu pro duplikace mezi servery prostřednictvím rozšíření Galera. Pro duplikaci dat je vhodné využít softwarové RAID řešení.

5.2.3 Spolupráce mezi zaměstnanci, práce na dokumentech

OwnCloud poskytuje více možností spolupráce, které pokrývají tvorbu a editaci dokumentů, organizaci času nebo rozdělení pravomocí. Podobně jako Google Docs i ownCloud poskytuje spolupráci na dokumentech mezi více uživateli v reálném čase. Výhodou je, že dokumenty jsou ukládány do open source formátu odt.

Dokumenty je možné sdílet s jednotlivci anebo celými skupinami. Úpravy různých uživatelů jsou graficky rozlišeny. OwnCloud je připraven i na situace, kdy dojde k nechtěnému smazání dokumentů, systém průběžně ukládá revize úprav a lze se vracet k předchozím verzím a to neomezeně.



Obrázek 5.3: Rozlišení úprav uživatelů ownCloudu při práci ve sdíleném dokumentu

S verzováním souborů souvísí i možnost monitorování jejich úpravy. Jeden z dílčích modulů umožňuje sledovat kdo, kdy a jak upravil daný soubor, komu ho sdílel, nebo kdo ho smazal.

Jak bylo výše uvedené, výsledné dokumenty se ukládají ve formátu odt, který přímo podporuje kancelářská sada Libre Office, která je v podniku často používána pro editaci dokumentů, protože funguje na operačních systémech Windows i Mac OS X, což jsou nejvíce využívané systémy ve firmě.

5.2.4 Sdílený kalendář a to-do list

Další ze silných stránek ownCloudu je kalendář. Každý uživatel si může vytvořit až několik kalendářů a sdílet je s ostatními. Také je možné povolit úpravu vlastního kalendáře jiným uživatelem, nebo naopak kalendář zpřístupnit jen pro čtení. Pro účely daného podniku bude při konfiguraci vhodné vytvořit hned několik kalendářů. Po uvedení systému ve firmě bude moci každý uživatel vytvářet své kalendáře, které může sdílet s jednotlivými spolupracovníky nebo skupinami spolupracovníků.

OwnCloud disponuje i rozšířením pro správu to-do listů, které lze spravovat a používat podobně jako kalendář.

5.2.5 Sdílení souborů

OwnCloud je primárně vytvořený pro synchronizaci a sdílení souborů a poskytuje větší škálu možností při sdílení než jeho největší konkurenti. Kromě běžného sdílení je možné také nastavit přístupové heslo, případně povolit do sdílené složky nahrávání souborů uživatelům, kteří nemají účet na ownCloudu. To je ideální možnost, jak získat například podkladové materiály od zákazníků nebo externích zaměstnanců, které jsou tak velké, že použití mailu nepřichází v úvahu.

5.2.6 Správa uživatelů

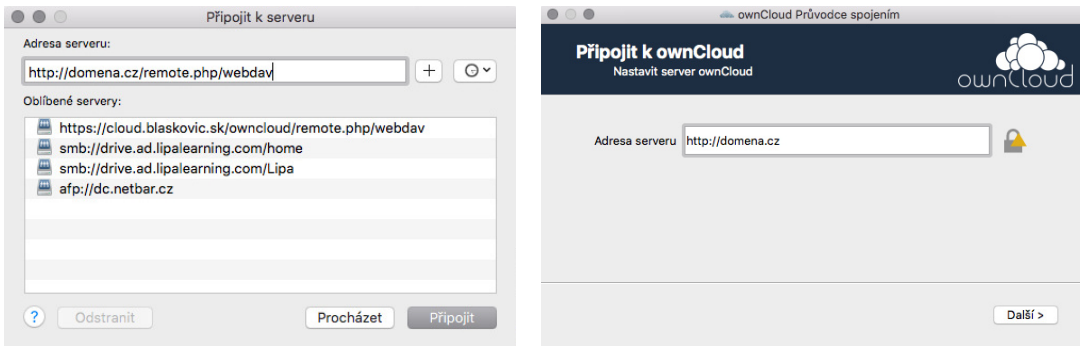
Správa uživatelů je na vysoké úrovni a dovoluje vytváření skupin, nastavení administrátorů pro danou skupinu a mnoho dalšího. Díky těmto možnostem je možné oddělit od sebe například uživatele různých oddělení ve firmě a udělit možnost práva administrace daného oddělení konkrétnímu zaměstnanci.

5.2.7 Integrace

Nejdůležitější součástí všech cloudových řešení je možnost integrace do různých zařízení, aby službu mohl využívat každý uživatel nezávisle na tom, jaké zařízení a systém používá. Protože se jedná o open source řešení s veřejným protokolem, existuje tu i možnost integrace do mnoha dalších systémů.

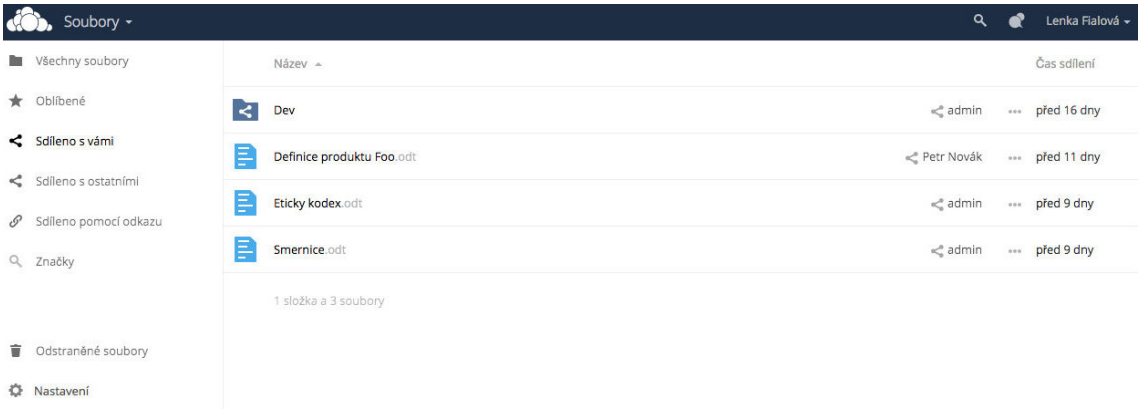
OwnCloud disponuje klientskými desktopovými aplikacemi pro Microsoft Windows, Mac OS X a většinu Linuxových distribucí. Dále lze k systému přistupovat pomocí webového rozhraní nebo využít aplikace pro mobilní platformy Android a iOS, a dokonce ve více variantách pro různé použití.

Desktop klienti Základní klient pro synchronizaci souborů má jednoduché nastavení. Stačí zadat adresu ownCloudu serveru, přístupové údaje a zvolit adresáře ke sdílení. Pro účely našeho podniku je vhodné zvolit všechny složky, ale obecně lze vybrat jen relevantní složky, případně ze synchronizace vyloučit některé podsložky.



Obrázek 5.4: Postup připojení desktopového klienta na systému Mac OS X

Webový klient V případě využívání systému na pracovišti, budeme preferovat přístup k ownCloudu pomocí pokročilého webového rozhraní, přes které lze nahrávat, prohlížet, sdílet a organizovat soubory.



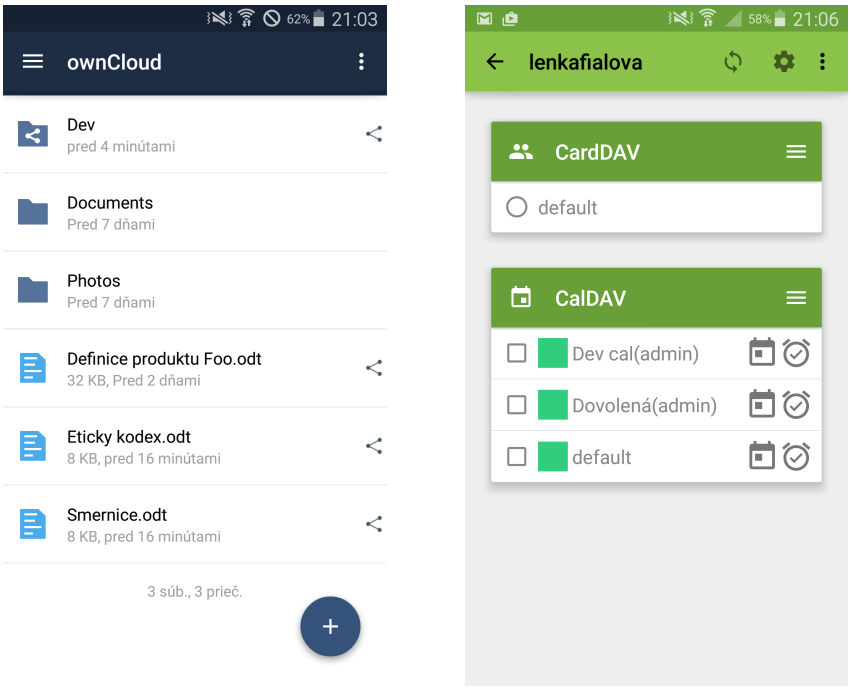
Obrázek 5.5: Webový klient ownCloudu

Mobilní klienti Při práci z domova lze přistupovat k firemním datům i například pomocí vlastních nebo firemních mobilních zařízení. K tomuto účelu existuje pro zařízení se systémem Android i iOS mobilní aplikace ownCloud. Verze pro systémy Android je dostupná například na Google App Play Store za cenu 20,37 Kč. Poplatek za aplikaci umožňuje podpořit vývojáře open source řešení, nicméně aplikace je dále dostupná i bezplatně na aplikačním marketu F-Droid [1]. Mobilní verze ownCloud klienta pro mobilní zařízení značky Apple, tedy zařízení se systémem iOS, je dostupná na AppStore za cenu 0,99$.

Mobilní klienti jsou obecně na vysoké úrovni. Lze plnohodnotně prohlížet soubory ze sdíleného úložiště. Do zařízení se přitom nesynchronizují všechna data, ale prohlížení funguje na principu podobném prohlížení webových stránek. Soubory se fyzicky stahují do mobilního zařízení až při jejich otevření. Pokud by ale přesto bylo třeba některá data v mobilních zařízeních synchronizovat neustále, mobilní aplikace to umožňuje. Dokonce je možné si zvolit, zda se mají data synchronizovat vždy při dostupném internetovém připojení nebo jen při připojení přes Wi-fi síť.

[1] F-Droid je aplikační market pro systémy Android, který nabízí jen open source a bezplatné aplikace.

Bohužel mobilní aplikace ownCloud podporuje jen práci se soubory. Synchronizovat kontakty a kalendáře je možné prostřednictvím protokolů CalDAV a CardDAV, jak bude uvedeno v další kapitole. Tento způsob lze využít i v případě mobilních aplikací. Příkladem mobilní aplikace, která využívá protokoly CalDAV a CardDAv je DAVdroid, která je dostupná zdarma ke stažení na F-Droid marketu.



Obrázek 5.6: Rozhraní mobilních aplikací ownCloud a DAVdroid

5.2.8 WebDAV, CardDAV, CalDAV

OwnCloud řešení nabízí podporu WebDAV pro soubory, CardDAV pro kontakty i CalDAV pro kalendář. To dovoluje uživatelům ownCloud importovat do každé aplikace, která zmíněné standardní protokoly podporuje. Mezi takové aplikace patří například Outlook DAV Client (Windows), CloudNotes (Mac OS X) nebo GNOME Online Accounts (Linux s prostředím Gnome). Pokud z nějakého důvodu na počítači nechceme oficiální aplikaci synchronizace ownCloudu, lze adresářovou strukturu připojit jako další síťový disk přes protokol WebDAV. Je třeba si ale uvědomit, že takto připojený disk je jen síťový, a tak k prohlížení a editaci dokumentů na tomto disku je potřeba internetové připojení. Přináší to velkou výhodu tím, že soubory nezabírají místo na pevném disku, na druhou

stranu v případě výpadku připojení nelze k souborům přistoupit. Kalendář je sice možné synchronizovat přes protokol CalDAV, ale pro potřeby daného podniku se bude využívat přístup ke kalendářům pomocí webového rozhraní a k přístupu přes mobilní zařízení se bude využívat příslušná synchronizace zmíněná v předešlé kapitole.

5.2.9 LDAP / ActiveDirectory

Množství podniků používá pro organizaci zaměstnaneckých účtů komunikační protokol LDAP nebo službu pro správu počítačové sítě Active Directory. Aby nedocházelo k redundanci dat, ale správa uživatelů zůstala jednoduchá, není potřeba všechny účty duplikovat do ownCloudu. Ten totiž podporuje jak LDAP, tak i Active Directory a dokáže pomocí nich autentifikovat své uživatele.

V současné době tuto možnost zatím nevyužijeme, protože podnik zatím LDAP nenasadilo. Vzhledem k tomu, že se ale podnik neustále rozrůstá, dá se očekávat, že se v budoucnu centrální LDAP server zavede. OwnCloud tuto funkcionalitu plně podporuje, takže není třeba mít obavy, že by firma v tomto směru narazila na problémy.

5.2.10 Další možnosti rozšíření

Pro ownCloud existuje množství různých pluginů, které rozšiřují jeho základní funkcionalitu. Instalace je snadná, takže je možné si poměrně jednoduše svůj ownCloud přizpůsobit vlastním potřebám přidáním doplňujících funkcí. Dále je možné si vytvořit vlastní rozšíření, které bude šité na míru přímo pro podnik. Obecným příkladem může být automatická synchronizace s programy pro účetnictví nebo s docházkovým systémem.

Protože se jedná o open source nástroj, jehož vývoj probíhá na GitHub [2], tak případné chyby lze okamžitě nahlásit a v krátké době získat dočasné řešení od vývojářů nebo široké komunity, dokud nebude vydán update v nejbližší verzi, kde bude chyba opravena.

Komunita stojící za ownCloudem je opravdu velká a o systém se stará rozsáhlý tým vývojářů. Pozorováním jsem zjistila, že příspěvky do kódu často vývojáři převezmou a

[2] GitHub je webová služba podporující vývoj softwaru za pomocí verzovacího nástroje Git. Zahrnuje bezplatný webhosting pro open source projekty.

zapracují do oficiální verze ownCloudu. Protože podnik, do kterého systém nasazuji má mezi zaměstnanci tým programátorů, dá se očekávat, že pokud by firmě nějaká funkcionalita chyběla, podnik ji dokáže doimplementovat svépomocí. Dokonce lze takové rozšíření nabídnout i upstreamu [3], kteý ji může přidat do hlavní verze ownCloudu. Takovým způsobem se podnik začne nejen spolupodílet na vývoji open source projektu, ale zároveň získá podporu nové funkcionality od vývojářů ownCloudu a do budoucna nebude třeba přidanou funkcionalitu ladit pro každou nově vydanou verzi systému.

5.2.11 Instalace ownCloud serveru

Podnikový linuxový (Debian 8) server má již nainstalován webový server Apache, databázový systém MariaDB i PHP a příslušné PHP moduly, které jsou pro chod ownCloudu nezbytné. Instalaci budu provádět přes příkazový řádek.

V případě, že by server nebyl takto připraven, je třeba doinstalovat kompletní LAMP server [4]. Doinstalování těchto prerekvizit je možné například tímto způsobem:

```
apt-get install apache2 mariadb-server libapache2-mod-php5
apt-get install php5-gd php5-json php5-mysql php5-curl
apt-get install php5-intl php5-mcrypt php5-imagick
```

Pokuž je již připraven funkční webový server s databází MariaDB a podporou pro PHP aplikace, je třeba si stáhnout poslední verzi ownCloud serverové aplikace z internetu například tímto způsobem:

Přejdu do adresáře html, kde se nachází Apache:

```
cd /var/www/html
```

Zahájím stahování poslední dostupné verze 9.0.1:

```
wget https://download.owncloud.org/community/owncloud-9.0.1.tar.bz2
```

Vyextrahuji stažený archiv a poté ho smažu:

```
sudo tar -xvf owncloud-9.0.1.tar.bz2 -C /var/www/html/
sudo rm owncloud-9.0.1.tar.bz2
```

[3] Upstream je místo, kde probíhá hlavní vývoj open source nástroje.

[4] LAMP je model řešení webových služeb, název je zkratkou pro Linuxový operační systém, webový server Apache, databázový systém MySQL/MariaDB a skriptovací jazyk PHP. [15]

Nastavím patřičná oprávnění www-data na složky html a owncloud:

```
sudo chown www-data:www-data -R /var/www/html
sudo chown www-data:www-data -R /var/www/html/owncloud
```

Poté je potřeba se přihlásit do databázového systému MariaDB, vytvořit uživatele a databázi pro ownCloud:

```
mysql -u root -p

MariaDB [root]> CREATE USER 'username'@'localhost' IDENTIFIED BY '
   password';
MariaDB [root]> CREATE DATABASE IF NOT EXISTS owncloud;
MariaDB [root]> GRANT ALL PRIVILEGES ON owncloud.* TO 'username'@'
   localhost' IDENTIFIED BY 'password';
MariaDB [root]>> FLUSH PRIVILEGES;
MariaDB [root]> exit
```

Dále provedu ověření, zda uživatel má přístup k vytvořené databázi. Pokud je databázový server nainstalovaný na stejném systému, použiju příkaz:

```
mysql -uUSERNAME -p
```

Pokud je na jiném systému, spustím s parametrem hostname:

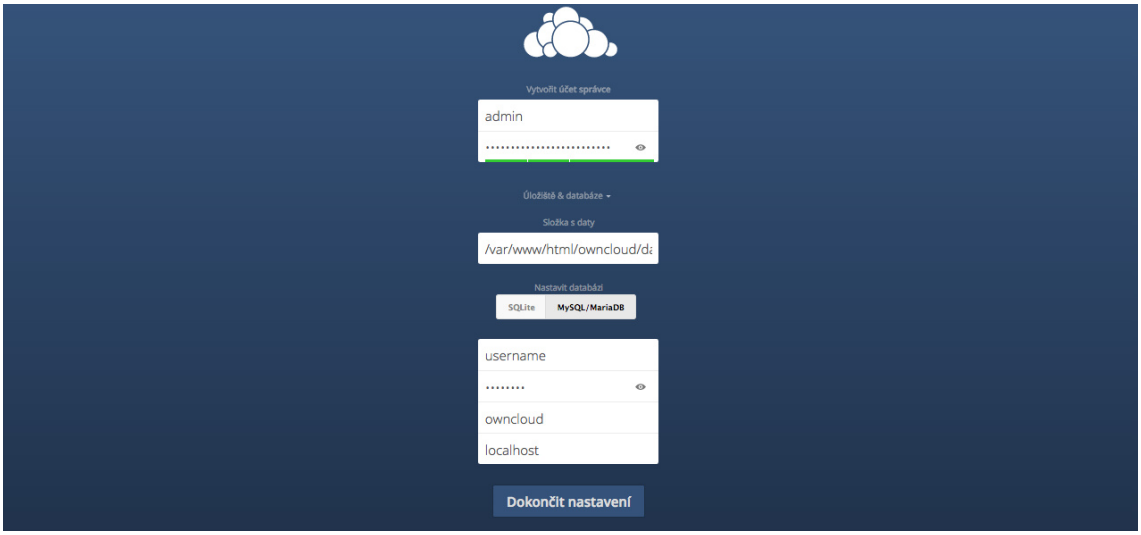
```
mysql -uUSERNAME -p -h HOSTNAME
```

Mělo by se zobrazit:

```
MariaDB [root]> SHOW VARIABLES LIKE "version";
+---------------+--------+
| Variable_name | Value  |
+---------------+--------+
| version       | 5.1.67 |
+---------------+--------+
1 row in set (0.00 sec)
MariaDB [root]> quit
```

Nyní v prohlížeči na adrese http://localhost/owncloud vložím přihlašovácí jméno a heslo administrátora a potvrdím tlačítkem Dokončit nastavení.

OwnCloud server je v tuto chvíli již připraven k použití, další administraci podnikového cloudu provádí administrátor pomocí těchto údajů.



Obrázek 5.7: Dialog vytvoření administrátorského účtu

5.2.12 Konfigurace

Věškerou konfiguraci je možné jednoduše realizovat prostřednictvím webového rozhraní. Po přihlášení je vidět v pravém horním rohu možnost vstoupit do nastavení, kde lze spravovat uživatele, zapínat a vypínat doplňkové aplikace či rozšíření nebo nastavovat základní pravidla pro ownCloud.

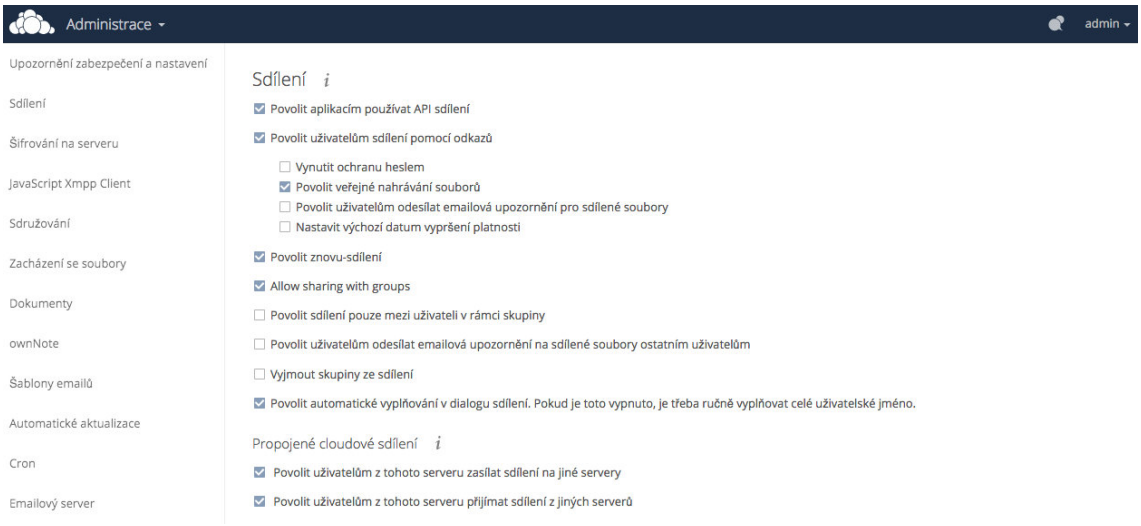
Pod položkou uživatelé lze přidávat nové uživatelské účty, přidělovat jim kvóty na diskový prostor a rozdělovat je do skupin. Uživatelé ve stejné skupině uvidí přihlašovací jména všech ostatních uživatelů v dané skupině a budou moci mezi sebou jednoduše sdílet vybrané soubory, kontakty či kalendář. V menu aplikace se nachází správa instalovatelných zásuvných modulů. K dispozici je seznam zhruba 30 předinstalovaných doplňků, které lze jedním kliknutím zapnout nebo vypnout. Přímo z tohoto webového rozhraní se instalují také další doplňky, které si lze stáhnout z internetu. Pod tlačítkem Admin se nachází obecné nastavení ownCloudu. Zde je možné nastavit limity velikosti souborů, exportovat/importovat nastavení a uživatele nebo upravit nastavení šifrování.

V případě našeho podniku je potřebné vytvořit účty všech zaměstnanců firmy a přidělit jim počáteční heslo. Dále je potřeba provést různá nastavení.

Základním nastavením je nastavení sdílení ownCloudu, zpřístupnění možností sdílení zaměstnanců apod. Je třeba správně nastavit práva zaměstnancům na sdílení souborů i povolení veřejného nahrávání.

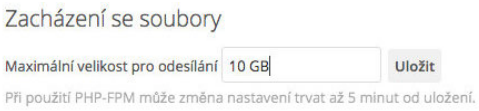
V dalším kroku povolíme tzv. „Federated Cloud Sharing“, což je sdílení dat mezi různými instancemi ownCloudu. Tím se povoluje možnost zaslat sdílený soubor přes odkaz jinému uživateli, který si může soubor přidat do vlastní instance ownCloudu.

V defaultním nastavení nebudu zaměstnance nutit při sdílení udávat heslo, protože častokrát to není potřeba a pokud to bude nutné, zaměstnanec si tuto možnost může zvolit sám. Všeobecné nastavení sdílení je na následujícím obrázku 5.8.



Obrázek 5.8: Obecné nastavení sdílení v ownCloudu

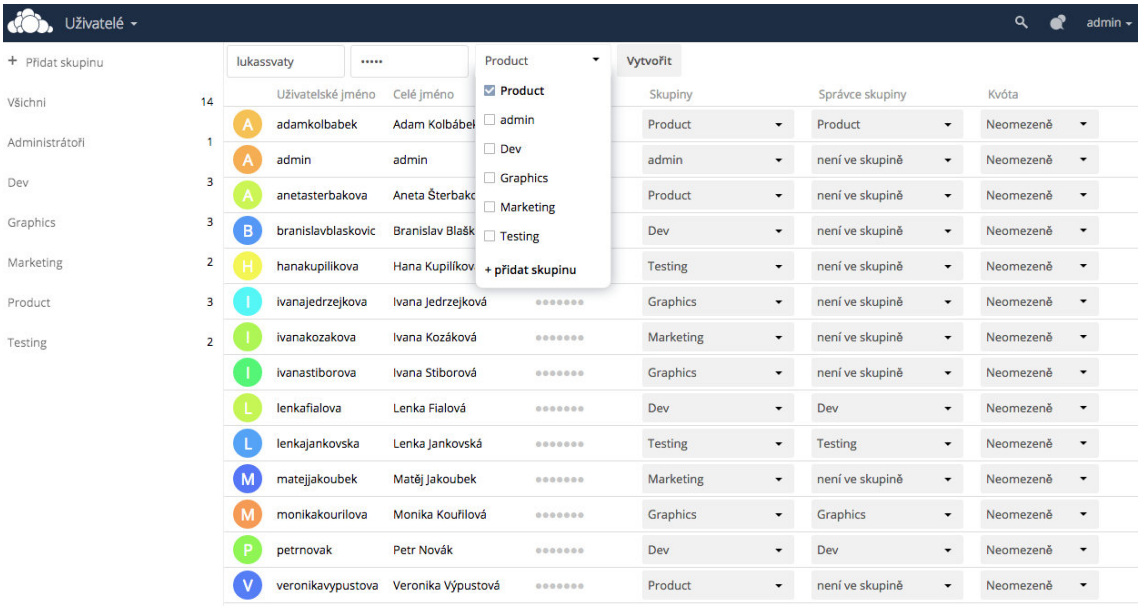
OwnCloud má v základním nastavení povolený upload maximální velikosti souboru do 2MB. Tuto hodnotu je třeba pro účely daného podniku navýšit na 10 GB, nastavení přímo v rozhraní ownCloudu je vidět na obrázku 5.9.



Obrázek 5.9: Nastavení limitu pro velikost uploadovancýh souborů

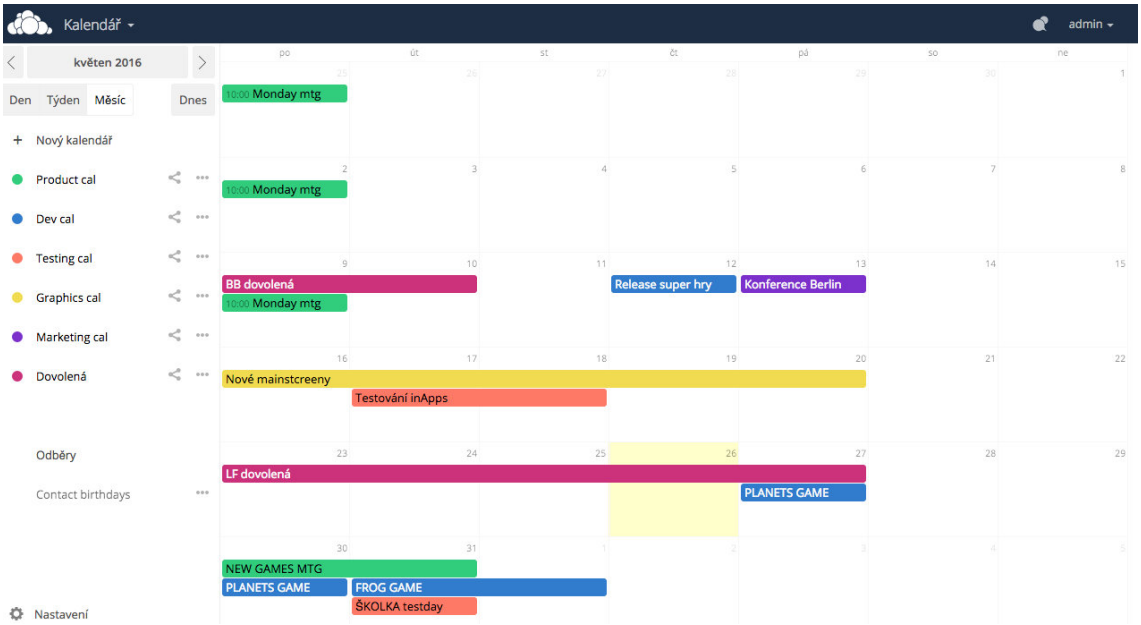
Dalším nastavením jsou uživatelské skupiny. Toto nastavení lze najít pod položkou Uživatelé v menu administrátora. Nejprve je vhodné vytvořit základní skupiny, které ko-

respondují s rozdělením ve firmě. Dalším krokem je pro každé oddělení vytvořit zaměstnanecké účty a pro každou skupinu zvolit administrátora, který může spravovat nastavení v rámci této skupiny. Administrátorem je vždy manažer daného oddělení. Příklad vytvořené struktury uživatelů podniku je znázorněn na obrázku 5.10.



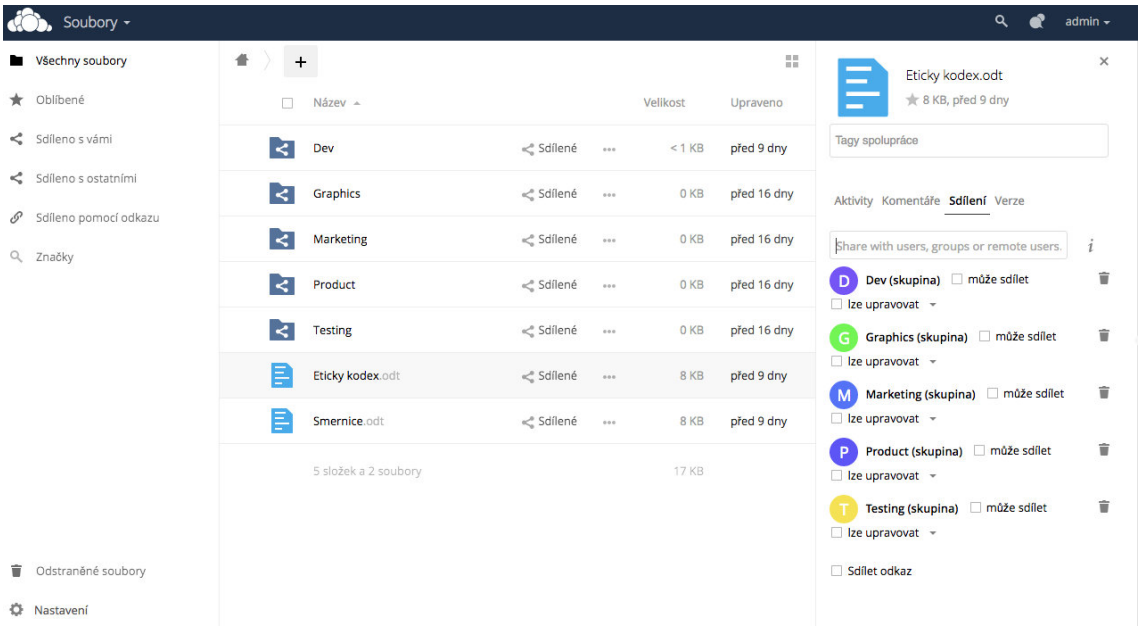
Obrázek 5.10: Nastavení správy uživatelů a skupin

Dále je třeba pro potřeby podniku vytvořit sdílené kalendáře. Podobně jako jsou zaměstnanci rozděleni do skupin podle oddělení, jsou i kalendáře vytvořeny tímto způsobem. Dále je vytvořen společný kalendář pro celou firmu, který je určen pro zápis dovolené. Každý uživatel si může vytvořit i své vlastní kalendáře a sdílet je s jinými zaměstnanci. Příklady záznamů v podnikovém kalendáři jsou vidět na obrázku 5.11.



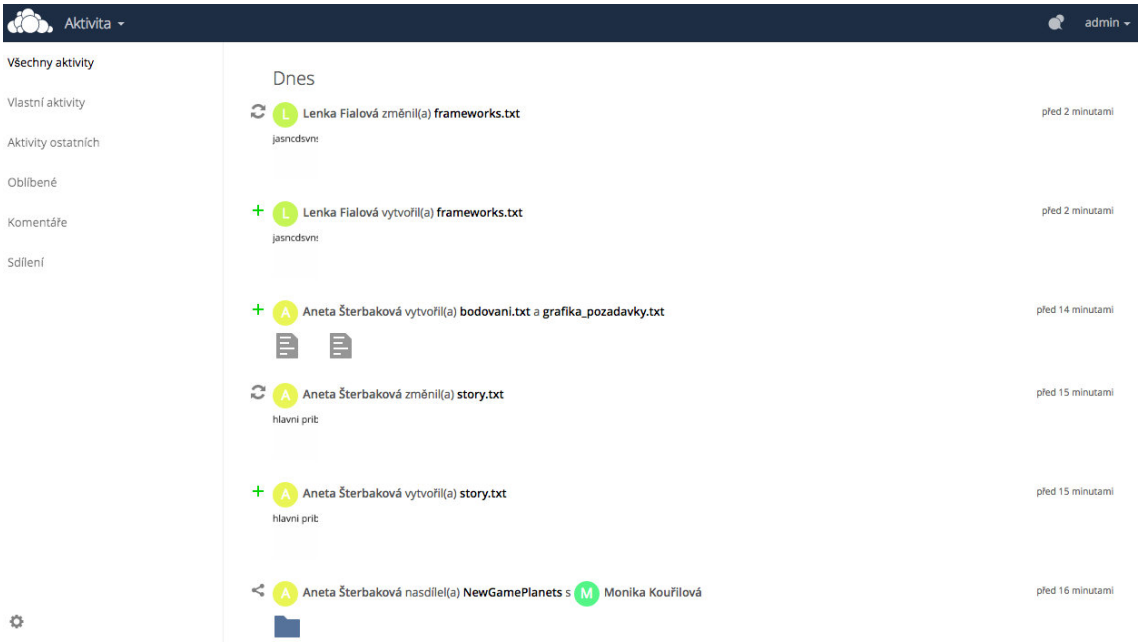
Obrázek 5.11: Náhled na kalendáře v prostředí ownCloudu

Firma by ráda některé dokumenty sdílela napříč všemi odděleními. Takovými soubory jsou například etický kodex a směrnice firmy. Po vytvoření dokumentů se nastaví sdílení se všemi odděleními, aby je mohli prohlížet všichni zaměstnanci, zároveň ale znemožníme editaci těchto souborů. Toto nastavení znázorňuje obrázek 5.12.



Obrázek 5.12: Nastavení sdílených dokumentů v prostředí ownCloud

Jeden z požadavků byl, aby vedení firmy mělo přehled o změnách. OwnCloud toto poskytuje a mimo to vidí každý svoji vlastní aktivitu i aktivitu ostatních zaměstnanců, s kterými spolupracuje na stejných dokumentech. Změny dokumentů jsou seřazeny chronologicky v „activity logu“ a obsahují informace kdo, co a kdy změnil. Náhled na activity log nabízí obrázek 5.13.



Obrázek 5.13: Náhled na výpis aktivit v prostředí ownCloudu

Používání ownCloudu je velmi intuitivní, přesto je vhodné, aby byla svolána informační schůzka, kde bude zaměstnancům vysvětlen postup přihlášení a možnosti, které ownCloud nabízí. Součástí této schůzky bude i předání listiny každému zaměstnanci, kde se dozví své počáteční heslo a podpisem se zaručí, že své heslo změní v daném časovém intervalu.

V budoucnu je třeba pro zajištění bezpečnosti v případě přístupu z domova zavést připojení pomocí VPN nebo povolit jen přístup přes HTTPS šifrovaný protokol, který vyžaduje vygenerování SSL certifikátu.

5.3 Analýza rizik

V této části práce je vypracována analýza rizik. Je dodržen postup, který nabízí metoda RIPRAN. První podkapitola 5.3.1 se zabývá odhalením možných hrozeb souvisejících s nasazením nového systému. Identifikovaná rizika slouží jako podklad pro navazující podkapitolu 5.3.2, kde je stanovena úroveň hrozeb a zranitelností. Na ni navazuje podkapitola 5.3.3, která se zabývá návrhem opatření proti definovaným rizikům. V poslední podkapitole 5.3.4 jsou vhodně interpretovány výsledky rizikové analýzy.

5.3.1 Identifikace rizik

Prvním úkolem analýzy rizik je stanovit jednotlivá rizika a přiřadit k nim scénář, který mohou vyvolat. Podkladem pro identifikace byly popis projektu, požadavky na nový systém, prognózy možných vnitřních a vnějších vlivů a zkušenosti s podobným typem projektu.

Při hledání hrozeb projektu je využito rozdělení informační infrastruktury podle Molnára [16] na hardware, software, dataware, peopleware a orgware.

Rizika v oblasti hardware

- Krádež/poškození serveru - Při krádeži nebo poškození serveru může podnik trvale přijít o svá data. Nejedná se jen o ztrátu ukládaných dat prostřednictvím ownCloudu, ale také může dojít ke ztrátě informací ohledně nastavení serveru, konfigurace databáze apod.

- Výpadek serveru - Pokud jsou data uložena pouze na jednom serveru, tak při výpadku přestává fungovat synchronizace. Pokud například více uživatelů pracuje na stejném dokumentu, tak po obnovení spojení může dojít ke konfliktům.

Rizika v oblasti software

- Zanesení chyb do systému - Protože ownCloud má rychlý vývoj a zároveň jde o open source řešení, mohou nové aktualizace v sobě obsahovat chyby, které omezí funkcionalitu systému. Práce zaměstnanců tak nebude efektivní a může se zpomalit vývoj projektů.

- Nízká rychlost systému - Výsledné binární soubory vyvíjených her nebo grafické soubory jsou často příliš velké a jejich zápis na disk může trvat delší dobu. V případě více probíhajících zápisů najednou nemusí být rychlost rotačního disku dostatečná.

Rizika v oblasti dataware

- Nezabezpečená osobní zařízení - Zaměstnanci mají možnost si synchronizovat pracovní dokumenty do svých mobilních telefonů nebo tabletů, hrozí nebezpečí úniku citlivých dat v případě ztráty zařízení.

- Růst náročnosti správy účtů - Při větším nárůstu nových zaměstnanců nebo při změně pozic stávajících pracovníků firmy se zvedne časová náročnost správy uživatelských účtů. Při každé změně je potřeba upravit záznamy v systému.

Rizika v oblasti peopleware

- Nezastupitelnost administrátora - Pokud administrátor systému onemocní nebo ukončí pracovní činnost ve firmě neexistuje za něj náhrada a není možné spravovat systém.

- Neexistující nápověda IS - K používání ownCloudu zatím neexistuje oficiální manuál. Může se stát, že zaměstnanci nebudou schopni systém používat.

- Zaměstnanci nebudou využívat nový systém - Zaměstnanci budou dále využívat pro sdílení souborů USB disky nebo mailového klienta, management podniku tak nebude mít přehled nad prací zaměstnanců, což bylo jedním z cílů projektu.

Rizika v oblasti orgware

- Neoprávněná manipulace s daty - V případě špatně nastavených přístupových práv zaměstnancům může dojít k neoprávněné manipulaci s daty . Hrozí ztráta dat nebo šíření citlivých informací mezi nepověřené osoby.

5.3.2 Kvantifikace rizik

Druhá fáze analýzy má za cíl ohodnotit pravděpodobnost vzniku scénářů, velikost následných škod a určit míru rizika. Byla stanovena tabulka 5.1 pro ohodnocení pravděpodobnosti výskytu rizik a tabulka 5.2 hodnotící dopad rizik. Na jejich základě je sestaven přehled hodnot mnou stanovených rizik v tabulce 5.3. Úrovně rizik definuje matice významnosti vyjádřená tabulkou 5.4.

Hodnota	Pravděpodobnost výskytu rizika	Popis výskytu
(4; 5>	JISTÁ	Riziko se téměř vždy vyskytne nebo s pravděpodobností 90-100%
(3; 4>	PRAVDĚPODOBNÁ	Riziko se pravděpodobně vyskytne
(2; 3>	MOŽNÁ	Riziko se někdy může vyskytnout (např. za specifických podmínek)
(1; 2>	NEPRAVDĚPODOBNÁ	Riziko se někdy může vyskytnout, ale je to nepravděpodobné
<0; 1>	VYLOUČENÁ	Riziko se vyskytne pouze ve výjimečných případech a za specifických podmínek

Tabulka 5.1: Hodnocení pravděpodobnosti výskytu rizik

Hodnota	Dopad rizika	Popis dopadu
(4; 5>	KRITICKÝ	Situace zásadně omezí nebo ukončí provoz firmy
(3; 4>	VÝZNAMNÝ	Situace velmi nebezpečně ovlivňuje vnitřní i vnější chod firmy
(2; 3>	STŘEDNÍ	Situace nebezpečně ovlivní vnitřní i vnější chod firmy
(1; 2>	NEVÝZNAMNÝ	Situace omezuje vnitřní chod firmy
<0; 1>	ZANEDBATELNÝ	Situace sice negativně omezuje chod firmy, ale nezpůsobuje ztráty větší jak 5%

Tabulka 5.2: Hodnocení dopadu rizik

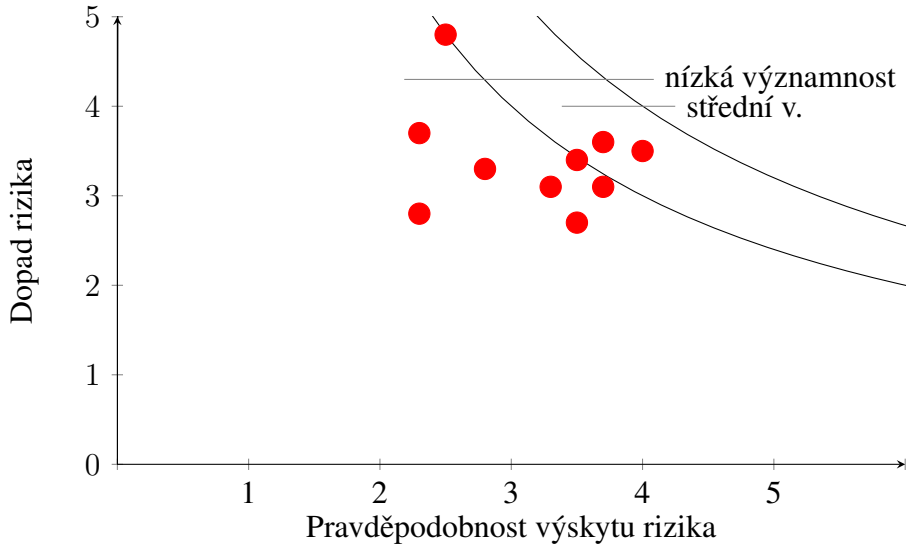
č.	Oblast	Riziko	P	D	H
1	HW	Krádež/poškození serveru	2,5	4,8	12
2	HW	Výpadek serveru	3,5	2,7	9
3	SW	Zanesení chyb do systému	3,7	3,1	11
4	SW	Nízká rychlost systému	2,3	3,7	9
5	DW	Nezabezpečená osobní zařízení	3,7	3,6	13
6	DW	Růst náročnosti správy účtů	4,0	3,5	14
7	PW	Nezastupitelnost administrátora	3,3	3,1	10
8	PW	Neexistující nápověda IS	3,5	3,4	12
9	PW	Zaměstnanci nebudou používat nový IS	2,3	2,8	6
10	ORW	Manipulace s daty vlivem nechráněného přístupu	2,8	3,3	9

Tabulka 5.3: Ohodnocení rizik

Hodnoty nalezených hrozeb jsou zaneseny do mapy rizik na obrázku 5.14. Většina hrozeb spadá podle matice ohodnocení do kategorie rizik s nízkou významností. Dvě rizika jsou na hranici nízké a střední významnosti a dvě rizika jsou středně významná. Z identifikovaných hrozeb žádná nespadá do kategorie s vysokou významností, tedy kategorie zcela neakceptovatelných rizik. Přesto budu pro všechna stanovená rizika hledat příslušná opatření, která by jejich hodnotu ještě snížila.

Dopady rizika							
	5	5	10	15	20	25	VYSOKÁ VÝZNAMNOST
	4	4	8	12	16	20	
	3	3	6	9	12	15	STŘEDNÍ VÝZNAMNOST
	2	2	4	6	8	10	
	1	1	2	3	4	5	NÍZKÁ VÝZNAMNOST
		1	**2**	**3**	**4**	**5**	
		Pravděpodobnost výskytu rizika					

Tabulka 5.4: Matice významnosti rizik



Obrázek 5.14: Mapa rizik

5.3.3 Návrhy opatření

Byla navržena následující opatření, která snižují hodnotu rizik a tedy zvyšují pravděpodobnost úspěšnosti projektu:

- Krádež/poškození serveru - Snížení dopadu rizika ztráty dat v případě porušení nebo krádeže serveru by vyřešily pravidelné zálohy na další server. Ideální formou je inkrementální záloha, která na rozdíl od plné zálohy zaznamenává pouze změny,

které proběhly od poslední zálohy a trvá tedy kratší dobu. Pro tyto účely lze využít nástrojů rear [5] nebo rdiff-backup [6].

- Výpadek serveru - Proti konfliktům vznikajícím v případě výpadku server se lze zabezpečit nasazením multi tenant řešení a využívat tak další server.
- Zanesení chyb do systému - Před každým updatem admnistrátor ověří novou verzi a provede testování.
- Nízká rychlost systému - Zvýšení rychlosti lze docílit výměnou disku na serveru za rychlejší SSD disk.
- Nezabezpečená osobní zařízení - Pokud zaměstnanec využívá přístup klientské aplikace ownCloudu ve svém osobním zařízení, bude zavedena povinnost používat antivirovou ochranu a zavést ochranný zámek pro přístup do zařízení.
- Růst náročnosti správy účtů - Tuto situaci by řešilo nasazení LDAP, které bude řešit automaticky přidávání nových uživatelů i řazení do skupin.
- Nezastupitelnost administrátora - Administrátor ownCloudu má jako jediný přístup ke správě systému. Je potřeba zvolit dalšího zaměstnance, kterému bude přidělen administrátorský účet a bude moci provádět správu systému v případě absence hlavního administrátora.
- Neexistující nápověda IS - Kvůli prozatím neexistující oficiální nápovědě k ownCloudu by bylo vhodné připravit manuál k použití a zaškolit zaměstnance.
- Zaměstnanci nebudou využívat nový systém - Management chce mít kontrolu nad probíhajícími projekty. Aby se zabránilo tomu, že nový systém nebudou zaměstnanci využívat, je třeba zavést jeho používání jako povinné.
- Neoprávněná manipulace s daty - Vhodným opatřením je zavést duální ověření přístupových práv, která jsou přidělována celým oddělením nebo jednotlivým zaměstnaneckým účtům.

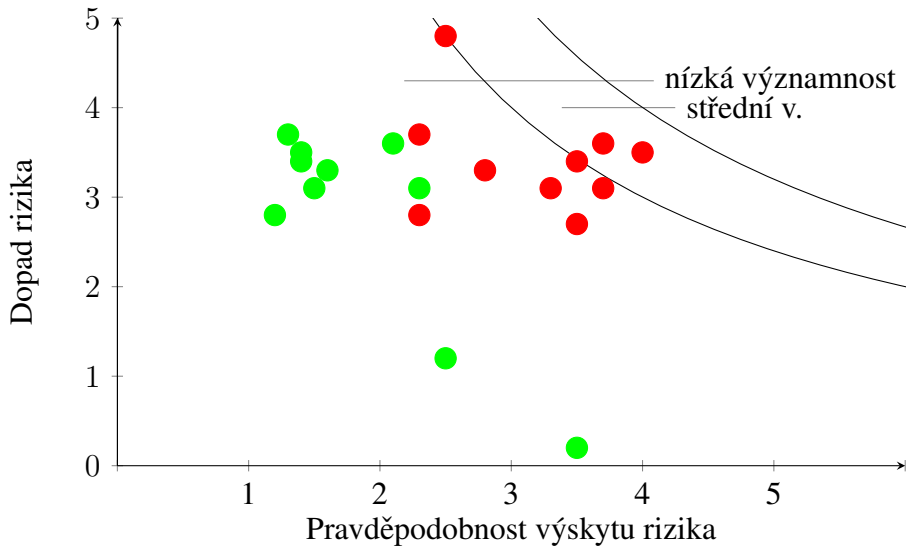
[5] Relax-and-Recover je nástroj pro bezúdržbovou tvorbu záloh Linuxových serverů.
[6] rdiff-backup je nástroj pro inkrementální zálohu zvolených adresářů.

S ohledem na tato opatření byla provedena nová kvantifikace rizik. Vliv opatření na hodnoty pravděpodobnosti a dopadu je zřejmý z následující tabulky 5.5.

č.	Navrhovaná patření	P’	D’	H’
1	Záložní server, pravidelné zálohy	2,5	1,2	3
2	Nasazení multi tenant řešení	3,5	0,2	1
3	Kontroly nových updatů	2,3	3,1	7
4	Nákup SSD disků	1,3	3,7	5
5	Povinné zabezpečení osobních zařízení	2,1	3,6	8
6	Zavedení LDAP	1,4	3,5	5
7	Rozšíření administrátorského přístupu na dalšího zaměstnance	1,5	3,1	5
8	Školení zaměstnanců	1,4	3,4	5
9	Zavedení povinnosti používat nový systém	1,2	2,8	3
10	Dvojitá kontrola přiřazení práv k účtům	1,6	3,3	5

Tabulka 5.5: Ohodnocení rizik po zavedení opatření

Nově ohodnocená rizika byla zanesena na původní mapu rizik. Výsledek je vidět na obrázku 5.15. Červené body znázorňují původní rizika, zelenou barvou jsou vyznačena rizika po zavedení opatření. Jak je z nové mapy rizik patrné, u všech hrozeb jsme dosáhli snížení hodnoty rizika, dokonce jsou nyní všechna rizika v intervalu nízké významnosti.



Obrázek 5.15: Mapa rizik po zavedení opatření

5.3.4 Výsledky analýzy rizik

Pro přehlednost výsledků analýzy rizik bylo využito textové interpretace metody RI-PRAN, která je doporučena v [1]. Efektivita navržených opatření a jejich vliv na hodnotu rizika jsou v závěru této kapitoly graficky vyjádřeny pomocí pavučinového grafu.

Pořadové číslo:	**I.**
Hrozba:	**Krádež/poškození serveru**
Scénář:	Ztráta uložených dat, ztráta dat nastavení
Pravděpodobnost:	Možná
Dopad:	Kritický
Hodnota rizika:	Střední
Návrh na opatření:	Záložní server, pravidelné zálohy
Snížená hodnota rizika:	Nízká

Pořadové číslo:	**II.**
Hrozba:	**Výpadek serveru**
Scénář:	Konflikty ve sdílených dokumentech
Pravděpodobnost:	Pravděpodobná
Dopad:	Střední
Hodnota rizika:	Nízká
Návrh na opatření:	Nasazení multi tenant řešení
Snížená hodnota rizika:	Nízká

Pořadové číslo:	**III.**
Hrozba:	**Zanesení chyb do systému**
Scénář:	Chybovost systému, nemožnost efektivně používat IS
Pravděpodobnost:	Pravděpodobná
Dopad:	Významný
Hodnota rizika:	Nízká
Návrh na opatření:	Zavedení kontroly nových updatů
Snížená hodnota rizika:	Nízká

Pořadové číslo:	**IV.**
Hrozba:	**Nízká rychlost systému**
Scénář:	Více probíhajících zápisů většího objemu dat způsobí snížení rychlosti systému, nemožnost efektivně používat IS
Pravděpodobnost:	Možná
Dopad:	Významný
Hodnota rizika:	Nízká
Návrh na opatření:	Pořízení SSD disků pro server
Snížená hodnota rizika:	Nízká

Pořadové číslo:	**V.**
Hrozba:	**Nezabezpečená osobní zařízení**
Scénář:	Únik citlivých dat
Pravděpodobnost:	Pravděpodobná
Dopad:	Významný
Hodnota rizika:	Střední
Návrh na opatření:	Povinné zabezpečení osobních zařízení
Snížená hodnota rizika:	Nízká

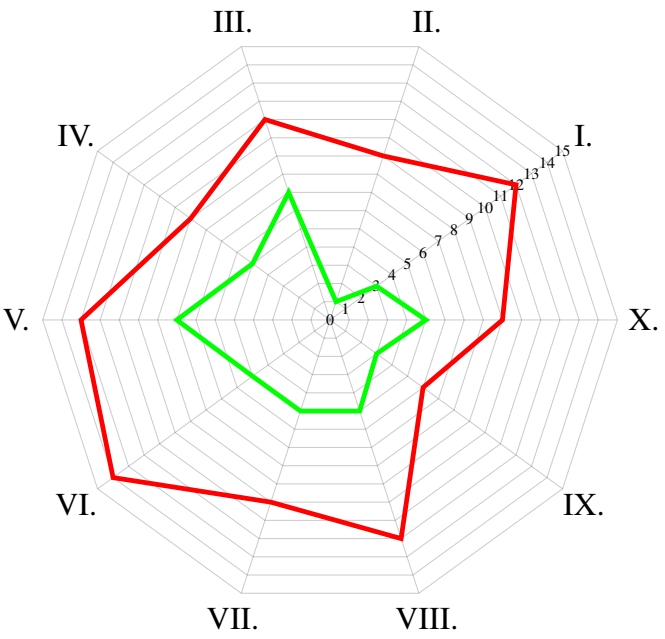
Pořadové číslo:	**VI.**
Hrozba:	**Růst náročnosti správy účtů**
Scénář:	Zpoždění úkolů souvisejících se správou účtů
Pravděpodobnost:	Jistá
Dopad:	Významný
Hodnota rizika:	Střední
Návrh na opatření:	Zavedení LDAP
Snížená hodnota rizika:	Nízká

Pořadové číslo:	**VII.**
Hrozba:	**Nezastupitelnost administrátora**
Scénář:	V případě absence administrátora nelze spravovat systém
Pravděpodobnost:	Jistá
Dopad:	Významný
Hodnota rizika:	Střední
Návrh na opatření:	Rozšíření administrátorského přístupu na dalšího zaměstnance
Snížená hodnota rizika:	Nízká

Pořadové číslo:	**VIII.**
Hrozba:	**Neexistující nápověda IS**
Scénář:	Zaměstnanci nebudou schopni systém používat
Pravděpodobnost:	Pravděpodobná
Dopad:	Významný
Hodnota rizika:	Střední
Návrh na opatření:	Školení zaměstnanců
Snížená hodnota rizika:	Nízká

Pořadové číslo:	**VIII.**
Hrozba:	**Zaměstnanci nebudou používat nový IS**
Scénář:	Zaměstnanci budou dále využívat pro sdílení souborů USB disky nebo maily
Pravděpodobnost:	Pravděpodobná
Dopad:	Střední
Hodnota rizika:	Nízká
Návrh na opatření:	Zavedení povinnosti používat nový systém
Snížená hodnota rizika:	Nízká

Pořadové číslo:	**X.**
Hrozba:	**Manipulace s daty vlivem nechráněného přístupu**
Scénář:	Ztráta dat, manipulace s daty nepověřeným zaměstnancem
Pravděpodobnost:	Možná
Dopad:	Významný
Hodnota rizika:	Nízká
Návrh na opatření:	Dvojitá kontrola přiřazení práv k účtům
Snížená hodnota rizika:	Nízká



Rizika:

I. Krádež/poškození serveru

II. Výpadek serveru

III. Zanesení chyb do systému

IV. Nízká rychlost systému

V. Nezabezpečená osobní zařízení

VI. Růst náročnosti správy účtů

VII. Nezastupitelnost administrátora

VIII. Neexistující nápověda IS

IX. Zaměstnanci nebudou používat nový IS

X. Manipulace s daty vlivem nechráněného přístupu

Obrázek 5.16: Vliv opatření na hodnotu rizika

Uvedená rizika jsou pouze ta nejvíce zřejmá a v rámci projektu je nutno počítat s tím, že se mohou objevit další hrozby. V rámci nasazení je třeba přiřadit zodpovědnost některému ze zaměstnanců firmy. Z hlediska zajištění opatření proti rizikům bude důležité si během plánování projektu zajistit finanční a časové rezervy.

Vzhledem k výsledkům rizikové analýzy je doporučena realizace projektu nasazení vybraného systému.

6 Závěr

Cílem této diplomové práce bylo vybrat a navrhnout nasazení privátního cloudového systému dle požadavků konkrétního podniku.

Úvodním úkolem bylo seznámit se s pojmem cloud v historickém i současném kontextu. Těchto znalostí jsem využila a s ohledem na potřeby firmy jsem vybrala tři možné technologie. Vzájemným porovnáním jsem z nich zvolila nejvíce vhodné řešení. V práci jsem dále popsala kroky instalace a konfigurace softwaru tak, aby si mohl tento systém nasadit podnik svépomocí.

Neméně důležitou částí bylo ověření, zda je zavedení cloudu vůbec vhodným krokem pro zmíněný podnik. K tomuto účelu jsem vypracovala studii příležitosti, která potvrdila, že cloudový systém bude pro firmu přínosem. Kromě zlepšení efektivity práce zaměstnanců, přispěje systém k rychlejší komunikaci a zvýší se úroveň zabezpečení dat v podniku.

V rámci práce jsem identifikovala možná rizika, která hrozí během nasazení cloudového systému do informační struktury firmy. Navrhla jsem opatření, která zajistí snížení dopadu rizik na přijatelnou úroveň.

Možnosti cílového cloudového řešení jsem v průběhu vypracování této práce konzultovala s vedoucími jednotlivých oddělení společnosti. Protože v rámci práce byly splněny všechny požadavky na systém, firma se rozhodla, že v blízké době tento projekt realizuje.

Výsledné řešení je možné v budoucnu dále rozvíjet. Jednou z možností je například obohacení funkcionality instalováním dalších dostupných rozšíření, případně si může firma naprogramovat vlastní funkční nadstavbu.

Seznam použitých zkratek

IaaS (Infrastructue as a Service) – Distribuční model Cloud Computingu zaměřený na poskytování ucelených infrastrukturních služeb

IS (Information System) – Informační systémy

IT (Information Technology) – Informační technologie

LDAP ((Lightweight Directory Access Protocol) – Protokol pro ukládání a přístup k datům na adresářovém serveru

LAMP (Linux Apache MySQL PHP) – Platforma pro implementaci dynamických webových stránek

NIST (National Institute of Standards and Technology) – Národní institut standardů a technologie, laboratoř standardů při ministerstvu obchodu Spojených Států.

PaaS (Platform as a Service) – Distribuční model Cloud Computingu zaměřený na poskytování prostředků pro vývoj a údržbu aplikací

RAID (Redundant Array of Inexpensive/Independent Disks) – Metoda zabezpečení dat proti selhání pevného disku

rear (Relax-and-Recover) – Nástroj pro zálohování serverů

RIPRAN (Risk Project Analysis) – Metoda pro analýzu projektových rizik

SaaS (Software as a Service) – Distribuční model Cloud Computingu zaměřený na poskytování softwaru

SLEPT (Social, Legal, Economic, Politic, Technological) – Metoda analýzu obecného okolí podniku

SSD (Solid-state drive) – Typ datového média

SWOT (Strengths, Weaknesses, Opportunities, Threats) – Metoda pro analýzu silných, slabých stránek, příležitostí a hrozeb (většinou podniku)

VPN (Virtual Private Network) – Virtuální privátní síť

XaaS (X as a Service) – „Cokoliv jako služba“, souhrnný pojem v informatice pro službově-orientovaný přístup k řízení a využívání informačních a komunikačních technologií formou služeb

Seznam obrázků

Seznam tabulek

Literatura

[1] DOLEŽAL J., B. LACKO, P. MÁCHAL a kolektiv. *Projektový management podle IPMA*. 2. vydání. Praha: Grada Publishing a.s., 2012. ISBN 978-80-247-4275-5.

[2] SMEJKAL V. a K. RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. vydání. Praha: Grada Publishing a.s., 2013. ISBN 978-80-247-4644-9.

[3] PESTLE analýza [online]. [cit. 2016-05-01]. Dostupné z: https://managementmania.com/cs/pestle-analyza

[4] Porterův model konkurenčních sil [online]. [cit. 2016-05-01]. Dostupné z: http://www.vlastnicesta.cz/metody/porteruv-model-konkurencnich-sil-1/

[5] McKinsey 7S Model: A strategic assessment and alignment model [online]. [cit. 2016-05-01]. Dostupné z: https://whittblog.wordpress.com/2011/04/24/mckinsey-7s-model-a-strategic-assessment-and-alignment-model/

[6] Model 7S - Mc Kinsey [online]. [cit. 2016-05-01]. Dostupné z: http://www.cie-plzen.cz/index.php/cz/lexikon-metod/model-7s-mc-kinsey

[7] MELL P. a T. GRANCE. The NIST Definition of Cloud Computing [online]. Gaithersburg: National Institute of Standards and Technology, 201. [cit. 2016-05-07]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[8] Co je to Cloud Computing a proč se o něm mluví [online]. [cit. 2016-05-01]. Dostupné z: http://www.businessvize.cz/software/co-je-to-cloud-computing-a-proc-se-o-nem-mluvi

[9] A Brief History of Cloud Computing [online]. [cit. 2016-05-07]. Dostupné z: http://www.nedocs.com/blog/history-of-cloud-computing

[10] The History of Cloud Computing [online]. [cit. 2016-04-27]. Dostupné z: http://www.eci.com/cloudforum/cloud-computing-history.html

[11] LACKO, Ľ. *Osobní cloud pro domácí podnikání a malé firmy*. Brno: Computer Press, 2012. ISBN 978-80-251-3744-4.

[12] VELTE A. *Cloud computing : praktický průvodce*. Brno: Computer Press, 2011. ISBN 978-80-251-3333-0.

[13] Phishing a pharming [online]. [cit. 2016-05-01]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

[14] SILOWASH G., CAPPELI D., MOORE A., TRZECIAK R., SHIMEALL T.J. a L FLYNN. Common Sense Guide to Mitigating Insider Threats 4th Edition [online]. Pittsburgh: Carnegie Mellon University, 2012 [cit. 2016-05-07]. Dostupné z: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

[15] LAMP (system bundle) [online]. [cit. 2016-05-01]. Dostupné z: https://en.wikipedia.org/wiki/LAMP_(software_bundle)

[16] MOLNÁR Z. *Efektivnost informačních systémů*. 2. vydání. Praha: Grada Publishing, 2001. ISBN 80-247-0087-5.

[17] BUYYA R., VECCHIOLA Ch. a S.T. SELVI. *Mastering cloud computing: foundations and applications programming*. San Francisco: Morgan Kaufmann Publishers Inc., 2013. ISBN 978-0-12-411454-8.